

ENHANCING CYBER RESILIENCE THROUGH INSURANCE REVISITING ANTI-BUNDLING REGULATION

SOPHIA MAURO

TAYLOR GROSSMAN

APRIL 2025



IST

Institute for
SECURITY + TECHNOLOGY

Enhancing Cyber Resilience through Insurance: Revisiting Anti-Bundling Regulation

April 2025

Authors: Sophia Mauro and Taylor Grossman

Design: Sophia Mauro

The Institute for Security and Technology and the authors of this report invite free use of the information within for educational purposes, requiring only that the reproduced material clearly cite the full source.

Copyright 2025, The Institute for Security and Technology
Printed in the United States of America



About the Institute for Security and Technology

Uniting technology and policy leaders to create actionable solutions to emerging security challenges

Technology has the potential to unlock greater knowledge, enhance our collective capabilities, and create new opportunities for growth and innovation. However, insecure, negligent, or exploitative technological advancements can threaten global security and stability. Anticipating these issues and guiding the development of trustworthy technology is essential to preserve what we all value.

The Institute for Security and Technology (IST), the 501(c)(3) critical action think tank, stands at the forefront of this imperative, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

We work across three analytical pillars: the **Future of Digital Security**, examining the systemic security risks of societal dependence on digital technologies; **Geopolitics of Technology**, anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries; and **Innovation and Catastrophic Risk**, providing deep technical and analytical expertise on technology-derived existential threats to society.

Learn more: <https://securityandtechnology.org/>

Acknowledgments

The Institute for Security and Technology (IST) is grateful for the support of Coalition, Inc., whose funding enabled us to pursue this line of research. We would especially like to thank Sezaneh Seymour and Daniel Woods for their invaluable feedback and expertise.

We are also grateful to the many individuals who contributed their time, perspectives, and expertise as we approached this piece, including Geoff Brown, Josh Corman, Michael Klein, Nick Leiserson, Michael Phillips, and Megan Stifel.



Contents

- Executive Summary1**
- Introduction 3**
- A Brief History of Cyber Insurance: The Connection Between Security and Insurance6**
 - Early Days of Cyber Insurance: Hands-On Security Assessments Aim to Mitigate Risk 6
 - Insurance for Data Breaches: Soft Markets Lead to Light-Touch Security Questionnaires 8
 - The Ransomware Era: New Forms of Security Assessment Emerge11
- Examining the Strategic Potential of Cyber Insurers15**
 - 1. A common goal 15*
 - 2. Addressing cyber risk with applicable security controls 15*
 - 3. Deeper risk insights 16*
- Towards Cybersecurity and Cyber Resilience: Security as a Requirement and as a Benefit 17**
 - Brandishing “Sticks”: Options for pursuing security as a requirement 18
 - Offering “Carrots”: Options for pursuing security as a benefit 20
 - Assessing Barriers and Concerns around Bundling 29
 - 1. Insolvency32*
 - 2. Risk Assessment and Pricing33*
 - 3. Discriminatory Practices35*
 - 4. Conflicts of Interest in Business-to-Business (B2B) Relationships.....36*
 - Bundling Today: Current barriers to adoption37
- Recommendations..... 40**
- Conclusion 43**

Executive Summary

Cyber threats pose a risk to organizations of all sizes and risk profiles. Small- and medium-sized enterprises (SMEs) and state, local, tribal, and territorial (SLTT) governments in particular face a unique set of challenges. SMEs and SLTTs may not understand the full extent of their exposure to cyber risk, may have less access to resources to protect themselves, or may not be prepared to defend themselves against attacks and respond should one occur.

Rather than relying solely on regulation like mandates and standards, market-based solutions could be another pathway towards helping to protect these vulnerable entities from costly cyber attacks. In particular, policymakers, business owners, and cybersecurity professionals alike have long envisioned cyber insurance as one such mechanism to improve general ecosystem-level security. While cyber insurance has become more common, most policies currently encourage consequence-management, rather than pre-breach cyber hygiene and resilience. Further, whereas most Fortune 500 companies hold cyber insurance policies, many SMEs and SLTTs have yet to obtain cyber insurance.

This paper examines the strategic potential of cyber insurers, who ultimately share a long-term goal with policyholders: reducing the impact and frequency of cyber incidents. Insurers also stand to gain from the unique access they have to breach data—in fact, they are one of the few actors in the ecosystem who can have visibility into and interpret the ways in which security controls impact security outcomes, namely through cyber insurance claims.

The report identifies requirements- and incentives-based approaches to strengthening security through insurance, focusing in particular on pre-breach security. It zeroes in on bundling as one incentive-based pathway toward enabling cyber resilience. Right now, traditional insurance policies can only provide reduced premiums at the time of underwriting or during the renewal process. A bundled security and insurance package might incorporate discounts or rebates into the security service, rewarding best practices or adoption of new cybersecurity systems over time. Bundling could also be uniquely tailored to the needs and risk profile of a specific company, such as an SME that may not qualify for security services from large vendors and could benefit from a security product or service that helps them to bolster their cybersecurity.

Thus far, bundling is not a prominent feature of the cyber insurance market, in part because the ecosystem is dominated by traditional insurance practices and hampered by an opaque regulatory regime. Bundling does raise important concerns around insolvency, risk visibility and pricing, anti-competitive behavior, and conflicts of interest from business-to-business

relationships. This paper examines each concern in turn, assessing the potential benefits and drawbacks of expanding the practice across the market. While these issues must be handled carefully, the insurance market has developed a robust set of tools—including prudential regulations and disclosure obligations—that can, if implemented correctly, help mitigate these concerns.

Ultimately, the report concludes with three main recommendations:

- 1. Regulators and policymakers should encourage cyber insurers to present policyholders with more proactive pre-breach risk mitigation tools and strategies, including by bundling insurance with security products and services;**
- 2. Researchers should conduct additional analysis to improve the understanding of bundling as a model, take a deep dive into a select few firms that offer bundled services and a few insured SMEs or SLTTs that have taken up those services, and explore why more firms do not; and**
- 3. Researchers should compare outcomes between states that allow bundling, and states that do not.**

While more investigation is needed, this report concludes that bundling is an important tool that should be considered in the cyber insurance market.

Introduction

“Imagine the future: Every business has network security insurance, just as every business has insurance against fire, theft, and any other reasonable threat. To do otherwise would be to behave recklessly as an executive and be open to lawsuits. Details of network security become check boxes when it comes time to calculate the premium. Do you have a firewall? Which brand? Your rate may be one price if you have one brand, and a different price if you have another brand. Do you have a managed security monitoring service? If you do, your rate is lower.”¹

- Bruce Schneier, “The Information Takeover”
February 2001

In 2001, Bruce Schneier heralded the eve of a new era in computer security, one in which cyber insurance would become synonymous with security. Businesses would no longer focus solely on identifying and avoiding threats, but instead on risk transfer, management, and mitigation. He saw a world in which insurance would offer reduced rates on premiums to those businesses with the most secure products, incentivizing the creation of more secure software, code, and products. As cyber insurance takes over, he argued, the marketplace would reward good security above all. Insurance would revolutionize cybersecurity—and cybersecurity would in turn revolutionize insurance.

Over two decades later, Schneier’s bold vision of a cyber insurance “takeover” has not (yet) come to pass. While reports estimate that 80% of large corporations hold cyber insurance, only 10% of small and medium-sized enterprises (SMEs) have adopted it.² Many scholars have argued that even for large companies that do purchase cyber insurance, the policies may not be priced accurately to reflect the potential systemic risks they face.³ Furthermore, the amount of money spent on cyber insurance remains insignificant compared to overall commercial

1 Bruce Schneier, “The Information Takeover,” *Information Security*, February 2001, https://www.schneier.com/essays/archives/2001/02/the_insurance_takeov.html.

2 “Reality check on the future of the cyber insurance market,” SwissRe, November 18, 2024, <https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html>.

3 Josephine Wolff, *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks* (Cambridge: The MIT Press, 2022), 4. In describing some of the novel challenges posed by cyber insurance, Wolff writes, “For instance, insurers had no obvious way to protect themselves against having to pay out claims to all of their cyberinsurance customers at once. It would be unheard of for an insurer’s entire customer base to simultaneously experience car accidents or health crises or natural disasters or robberies and file claims all at once. For risks like natural disasters that do affect large number of policyholders at once, insurers deliberately diversify their customers to be certain they are not all concentrated in any one place or demographic that might be hit especially hard specifically in order to avoid correlated losses.”

property and casualty (P&C) insurance, of which cyber insurance is a specialty line. According to one estimate, direct written premiums for cyber insurance totaled \$15.5 billion in 2024—only 1.6% of direct written premiums for global P&C insurance.⁴

Schneier also predicted that cyber insurance would, in essence, “solve” cybersecurity. With ransomware making headlines on a daily basis;⁵ new threats emerging, particularly as a result of AI and other emerging technologies;⁶ and increased targeting of critical infrastructure by adversaries, cyber threats continue to take a toll on lives, livelihoods, and national security. Cyber insurance has, to some extent, “solved” for ransomware and other data breaches by modeling the costs of cyber incidents; however, it is less clear that this consequence-led modeling approach appropriately factors in the vulnerability of insureds to incidents. If cyber insurance is to truly bolster ecosystem-wide cybersecurity, the marketplace incentive structure must encourage proactive cybersecurity, not just consequence-management, from the outset.

This incentive structure, as Schneier envisioned it, would come about through the reduction of premiums to reward insureds for selecting more secure products and services. Today, some insurers do indeed offer reductions on premiums based on a prospective insured’s use of a particular security service. In theory, this partnership, which we refer to in the paper as “co-marketing,” helps the insurer better assess a policyholder’s level of cybersecurity—and therefore their level of risk—through the underwriting process. However, current practices—including co-marketing, embedded policy features, and controls-based rate reductions—only play a role at the time of underwriting and renewal, not over the course of the policy.⁷ These partnerships encourage consequence-management, but may not incentivize the adoption of better cybersecurity from the outset. More importantly, these partnerships have yet to dramatically impact the resilience of the cybersecurity ecosystem.

What, then, is the current state of the cyber insurance market? How are insurers exploring options to incentivize their policyholders to implement security controls, thereby reducing incidents and claims? And what barriers prevent incentives from becoming more widespread in the marketplace? This report explores how cyber insurance can play a role in bolstering overall cybersecurity by unpacking one set of incentive structures: bundling.⁸ In this paper, bundling refers to the combination of an insurance product with a non-insurance, value-added product or service, offered at an additional cost, that helps to mitigate or manage loss. A

4 “Reality check on the future of the cyber insurance market,” SwissRe.

5 For more, see: “Ransomware Task Force,” Institute for Security and Technology, <https://securityandtechnology.org/ransomwaretaskforce/>.

6 For more, see: Jennifer Tang, Tiffany Saade, and Steve Kelly, “The Implications of Artificial Intelligence in Cybersecurity,” October 2024, <https://securityandtechnology.org/virtual-library/reports/the-implications-of-artificial-intelligence-in-cybersecurity/>.

7 IST assessed the offerings from the top 20 cyber insurers, as well as other smaller cyber insurers, to understand the current pre-breach mitigation measures offered by each and to determine whether any of them currently offer discounts.

8 “Cyber insurers” for the purposes of this paper refers to all insurance providers who offer cyber insurance, either as a dedicated, specialized offering or as one offering within a broader insurance portfolio.

policyholder may realize the benefits of bundling either by receiving a rebate on their premium when they adopt a new security service, or by receiving a reduced rate on the security service itself. By bundling cyber insurance with cybersecurity services, policyholders can better manage and mitigate their risk, reduce future claims, and even contribute to information gathering efforts to support further risk mitigation tactics.

Most fundamentally, cyber insurance constitutes risk management by collecting data through underwriting, pricing premiums, adding coverage exclusions, and verifying claims.^{9,10} In the aftermath of an incident, cyber insurers offer mitigation services like access to digital forensics and incident response firms (DFIR); legal, PR, and human resources aid; and other sources of expertise to help their insureds respond—decreasing the amount an insured might otherwise have to spend on recovery.¹¹ However, in many cases, post breach support is far from optimal. When it comes to support before a breach occurs, cyber insurers can do more to incentivize cybersecurity from the outset. Bundling is one example of a pre-breach loss mitigation strategy that could be a path towards enhancing cyber resilience through insurance.

First, in a brief history of the cyber insurance market over the last three and a half decades, this report explores the evolving connection between cybersecurity and insurance, including the use of security questionnaires, assessments, and network scans. It articulates the strategic potential of cyber insurers, who—given their pursuit of a common goal, capacity to access to deeper risk insights, and ability to match cyber risk with quality security controls¹²—could be well-placed to help businesses understand how to improve their cybersecurity. Next, the piece identifies requirements and incentives that could be implemented to strengthen the connection between insurance and cybersecurity, and ultimately help insurance play a role in risk management and mitigation before a breach occurs. It zeroes in on bundling, and assesses the barriers that may be preventing bundling from becoming a more common feature of the cyber insurance marketplace, as well as concerns the practice may raise. Finally, this report offers an agenda for future research and action by policymakers and regulators.

-
- 9 Carol Heimer, *Reactive Risk and Rational Action: Managing Moral Hazard in Insurance Contracts* (University of California Press, 1985); Omri Ben-Shahar and Kyle Logue, “Outsourcing Regulation: How Insurance Reduces Moral Hazard,” *Michigan Law Review* 111, 2 (2012), <https://repository.law.umich.edu/mlr/vol111/iss2/2>; Shauhin Talesh, “Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as “Compliance Managers” for Businesses,” *Law & Social Inquiry* 43, 2 (Spring 2018), <https://doi.org/10.1111/lsi.12303>.
- 10 Insurance, at its most basic level, indemnifies risk—that is, insurers agree to cover the cost of losses for a pool of insureds, making the cost of the loss more predictable through regular premiums paid by the insured to the insurer. Bob Blakley, Ellen McDermott, Dan Geer, “Information Security is Information Risk Management,” in *New Security Paradigms Workshop 2001*, New Mexico, September 11, 2001, <https://www.nspw.org/papers/2001/nspw2001-blakley.pdf>.
- 11 Talesh, “Data Breach, Privacy, and Cyber Insurance”; Jamie MacColl, James Sullivan, Jason R C Nurse, Sarah Turner, Gareth Mott, Edward Cartwright, and Anna Cartwright, “Cyber Insurance and the Ransomware Challenge,” Royal United Services Institute for Defence and Security Studies, July 2023, <https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-ransomware-challenge>.
- 12 Cyber risk is defined by NIST’s Computer Security Resource Center as the “risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions.” NIST, “Cyber Risk,” Computer Security Resource Center, last accessed April 2025, https://csrc.nist.gov/glossary/term/cyber_risk.

A Brief History of Cyber Insurance: The Connection Between Security and Insurance

Early Days of Cyber Insurance: Hands-On Security Assessments Aim to Mitigate Risk

Most observers trace the creation of the first cyber insurance policy back to 1995. Steven Haase, an insurance broker for a number of IT companies—including one firm generally credited with inventing online banking and a major network security company—noticed a gap in their insurance coverage. Despite carrying protection from other risks like auto accidents, liability for errors and omissions, employees who become injured or ill while working, or employees whose legal rights are violated, the companies did not have any protection from being held liable for the exposure of vast amounts of data in their systems. Over the course of the next two years, he and a colleague from AIG created the Internet Security Liability Policy, which AIG underwrote in April 1997.¹³

As Josephine Wolff describes, in 1997 the standard AIG Internet Security Liability Policy covered up to \$250,000 in legal costs and settlement fees, specifically protecting companies from legal costs associated with credit card data breaches.¹⁴ Haase explained the challenge of pricing a new form of risk in an interview later that year, saying “there aren’t really any actuarial studies of Internet commerce... Banks and other merchants aren’t too forthcoming with that sort of information.”¹⁵ To protect against that risk—and to attempt to incentivize better security for their policyholders—AIG offered a reduction on premiums for websites that had their security audited and certified by the National Computer Security Association, bringing the premium down from \$2,500 to \$1,875 annually.¹⁶

13 Wolff, *Cyberinsurance Policy*; Wells 2018; Andrew Granato and Andy Polacek, “The growth and challenges of cyber insurance,” The Federal Reserve Bank of Chicago, *Chicago Fed Letter* 426 (2019), <https://doi.org/10.21033/cfl-2019-426>.

14 Wolff, *Cyberinsurance Policy*.

15 Joshua Macht, “Safe Haase,” Inc Magazine, September 15, 1997, <https://www.inc.com/magazine/19970915/1427.html>.

16 Macht, “Safe Haase”; Wolff, *Cyberinsurance Policy*.

Other insurance companies soon followed suit. In 1999, CFC, then Click for Cover, launched a cyber policy covering data loss and hacking. Lloyd's of London too issued its first cyber insurance policy in 1999. By 2003, brokers and insurers including Chubb, Aon, Fidelity, Deposit, Marsh, Cigna, and Zurich had also introduced new policies covering cyber risk.¹⁷ The early years of cyber insurance—characterized by Daniel Woods and Josephine Wolff as the “experimental cyber” period—saw varying levels of coverage, relatively few policies issued, and low coverage limits.¹⁸

In this period, insurers managed a lack of data about overall levels of risk by conducting time-consuming, highly detailed security assessments of potential insureds.¹⁹ They not only assessed the security status of their insureds, but also offered premium reductions during the underwriting process to incentivize better security postures and more secure products. For example, amid ongoing vulnerability disclosures, J.S. Wurzler Underwriting Managers announced in 2001 that they would charge clients using Microsoft's Windows NT software 5 to 15% more on their premiums than those using different software. In a 2001 interview with founder and CEO John Wurzler, he cites extensive security assessments as the reason for this pricing, saying that the move was based on “findings from 400 security assessments that his firm has done on small and midsize businesses over the past three years.”²⁰ The J.S. Wurzler example is likely not the only case of a firm raising premium rates based on the use of a specific tool or service—however, lack of data makes it difficult to point to additional examples. During this same time period, AIG offered premium reductions to firms using Invicta Networks' security device. Explaining the rationale for offering the discount, AIG manager Ty Sagalow said, “We believe that our loss risk will be reduced through the software.”²¹ In another example, Lloyds of London gave customers a 10% reduction in their premiums if they purchased security software manufactured by Tripwire.²² Going a step further, insurer Hiscox in 2000 reportedly not only examined the security of a customer's internal security configurations in its assessments, but also looked at the security of its Internet service providers and other third party systems that their site used to price premiums.²³ As these examples illustrate, early underwriting for cyber insurance did not necessarily reflect a complete understanding of the

17 Lawrence Gordon, Martin Loeb, and Tashfeen Sohail, “A Framework for Using Insurance for Cyber-Risk Management,” *Communications of the ACM* 46, 3 (March 2003), <https://dl.acm.org/doi/10.1145/636772.636774>; Robert Bryce, “Windows raises hacking insurance prices,” *ZDNet*, May 29, 2001, <https://www.zdnet.com/article/windows-raises-hacking-insurance-prices/>; Jonathan Figg, “Cyber insurance to cover e-business,” *The Internal Auditor* 57, 4 (August 2000), <https://www.proquest.com/docview/202752959?sourcetype=Trade%20Journals>.

18 Daniel Woods and Josephine Wolff, “A history of cyber risk transfer,” *Journal of Cybersecurity* 11, 1 (2025), <https://doi.org/10.1093/cybsec/tyae028>.

19 Wolff, *Cyberinsurance Policy*.

20 Bryce, “Windows raises hacking insurance prices.”

21 Bryce, “Windows raises hacking insurance prices”; Irene Binal, “Former KGB spook plans to make the net totally secure,” *Silicon.com*, May 24, 2001, <https://www.zdnet.com/article/former-kgb-spook-plans-to-make-the-net-totally-secure/>.

22 Wolff, *Cyberinsurance Policy*, 47.

23 Wolff, *Cyberinsurance Policy*, 44; Figg, “Cyber insurance to cover e-business.”

specific services or controls that would lead to better cybersecurity for their policyholders; instead, these premium reductions demonstrate the exploratory, experimental nature of the period, characterized by frequent adoption of business-to-business relationships as insurers sought to decrease loss ratios.

Insurance for Data Breaches: Soft Markets Lead to Light-Touch Security Questionnaires

The cyber insurance market began to grow in the mid 2000s, largely in light of new data breach notification laws that required businesses to notify their customers in case of exposure.²⁴ Companies that had previously not paid attention to cyber insurance suddenly saw how consequential a breach could be in terms of technical investigations and breach notification costs, lawsuits and litigation, Federal Trade Commission (FTC) investigations, negative media attention, and more.²⁵ In addition to state-level data breach notification laws, in 2011 the Securities and Exchange Commission (SEC) issued guidance advising companies to publicly disclose their level of exposure to cybersecurity risk.²⁶ Together, these new regulations seem to have prompted more companies to seek out cyber insurance—albeit not at the rate predicted by optimistic onlookers in the early market. By 2011, the U.S. cyber insurance market was worth an estimated \$500 million,²⁷ up from less than \$100 million in 2002.²⁸ In comparison, the entire U.S. P&C market was worth an estimated \$249 billion in 2011.²⁹

Following a number of high profile destructive hacks, by 2015, the commercial cyber insurance market had nearly tripled to an estimated \$1.5 billion, and included approximately 44 different insurers who offered policies.³⁰ Combined, this resulted in a soft market—one where insurers

24 Wolff, *Cyberinsurance Policy*, 13-14. In 2003, California passed the first data breach notification law, mandating that companies report data breaches of personal information to those individuals involved. By 2007, 33 states had followed suit.

25 Wolff, *Cyberinsurance Policy*; Woods and Wolff, “A history of cyber risk transfer.”

26 Trey Herr, “Cyber insurance and private governance: The enforcement power of markets,” *Regulation & Governance* 15, 1 (January 2021), <https://doi.org/10.1111/rego.12266>; Wolff, *Cyberinsurance Policy*.

27 Aon, “Global Cyber Market Overview: Uncovering the Hidden Opportunities,” Aon Inpoint whitepaper, June 2017, <https://www.aon.com.au/australia/insights/reports-and-whitepapers/2017/global-cyber-market-overview-inpoint-report.pdf>.

28 Walter S. Baer and Andrew Parkinson, “Cyberinsurance in IT Security Management,” *IEEE Security & Privacy* 5, no. 3 (May/June 2007): 51, <https://ieeexplore.ieee.org/document/4218551>.

29 National Association of Insurance Commissioners, “U.S. Property & Casualty and Title Insurance Industries,” 2018, https://content.naic.org/sites/default/files/inline-files/topic_insurance_industry_snapshots_2018_mid_year_property_casualty_title_report.pdf.

30 Michael Menapace, “Examining the Evolving Cyber Insurance Marketplace,” written testimony before the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, March 19, 2015, <https://www.commerce.senate.gov/services/files/90FA0BC7-8686-4B90-9A1B-3525CC62D4FE>; Council of Insurance Agents & Brokers, “Cyber Market Watch Survey,” executive summary, April 2015, <https://www.ciab.com/wp-content/uploads/2015/04/CIAB-Cyber-Survey-Executive-Summary-April-20.pdf>; Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey,” executive summary, October 2015, https://www.ciab.com/wp-content/uploads/2017/04/Cyber-Market-Watch-Executive-Summary_FINAL.pdf; Aon, “Global Cyber Market Overview:

competed with one another for customers and market share, in turn driving premiums down. In addition, the scarce amount of data insurers did have about the levels of cyber risk for their insureds painted an optimistic picture: U.S. standalone cyber coverage loss ratios were only 48% in 2015.³¹ In comparison, the U.S. commercial property and casualty insurance net loss ratio averaged 69.3% in 2015.³²

As a result, insurers seem to have abandoned requiring time-intensive assessments and enforcing strict security requirements prior to issuing a policy.³³ The incentives of the market had shifted: insurers could no longer be as hands-on in assessing the full range of cyber risk if they wanted to keep up with the competition. Even with an expanding soft market, cyber brokers dealt with many uncertainties: in a 2015 survey of 44 respondents from 40 insurance brokerages, “60% of respondents do not ‘feel there is adequate clarity from both the specialist cybersecurity insurance market and traditional property casualty insurers as to what is covered and what is excluded.’”³⁴

Underwriting practices began to reflect these new dynamics. Insurance policies focused on one particularly high profile set of risks that were dominating headlines: data breaches. A 2017 study analyzed the content of 34 different insurance carriers’ questionnaires for prospective insureds filed between 2009 and 2016 in Pennsylvania, New York, and California.³⁵ The researchers found an emphasis on assessing the amount and type of data managed by the prospective insured. They note a lack of attention to security maturity, citing “little attention” to technical infrastructure, only one questionnaire that asked about the size of an organization’s information security budget, and no mentions of standard frameworks for IT management.³⁶ Likewise, the same study’s investigation of 96 pricing algorithms filed with U.S. regulators in Pennsylvania, New York, and California between 2009 and 2016 finds that pricing focused almost entirely on the amount and type of data with which a company dealt. Only 35% of the pricing algorithms used considered security when determining premium pricing, and most of this subset employed generic risk categories rather than specific information from the questionnaires.³⁷

Uncovering the Hidden Opportunities,” Aon Inpoint whitepaper, June 2017, <https://www.aon.com.au/australia/insights/reports-and-whitepapers/2017/global-cyber-market-overview-inpoint-report.pdf>.

31 Woods and Wolff, “A history of cyber risk transfer”; Fitch Wire, “US Cyber Insurance Sees Rapid Premium Growth, Declining Loss Ratios,” April 13, 2022, <https://www.fitchratings.com/research/insurance/us-cyber-insurance-sees-rapid-premium-growth-declining-loss-ratios-13-04-2022>.

32 National Association of Insurance Commissioners, “Report on the Cyber Insurance Market,” October 18, 2022, <https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf>.

33 Wolff, *Cyberinsurance Policy*; Daniel Woods and Tyler Moore, “Does Insurance Have a Future in Governing Cybersecurity?” *IEEE Security & Privacy* 18, 1 (Jan-Feb 2020), <https://www.computer.org/csdl/magazine/sp/2020/01/08833500/1dgc2GyFz1u>.

34 Council of Insurance Agents & Brokers, “Cyber Market Watch Survey,” April 2015.

35 Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, “Content Analysis of Cyber Insurance Policies: How do carriers price cyber risk?” *Journal of Cybersecurity* 5, 1 (2019), <https://doi.org/10.1093/cybsec/tyz002>.

36 Romanosky et al., “Content Analysis of Cyber Insurance Policies,” 12.

37 Romanosky et al., “Content Analysis of Cyber Insurance Policies.”

For example, one policy designated businesses as low, medium, or high hazard: low meant they conducted little to no business online, medium meant they partially conducted business via their website or retained sensitive digital information, and high meant that they conducted a large amount of business through their website or retained a lot of sensitive digital information.³⁸ Sometimes, rather than fill out a questionnaire, larger customers could secure coverage based on a phone call at the request of their broker. One underwriter participating in such a meeting, according to one survey study conducted, “suggested insurance could be bought without naming ‘who your dependencies are.’”³⁹

The Council of Insurance Agents and Brokers (CIAB) conducted a survey of 44 respondents from 40 insurance brokerages in 2015 to examine how underwriters in the cyber insurance market were assessing insureds’ cyber risk. The survey found that a majority of brokers—55% of those surveyed—reported that only a quarter of their clients had incorporated cyber risk into their enterprise risk management (ERM). An alarming 16% of brokers stated that none of their clients addressed cyber risk in their ERM.⁴⁰

This trend was equally troubling to insureds looking to lower their premiums through implementing good security practices. In 2015, a CEO of a small business testified before a U.S. Senate subcommittee about her experience renewing her business’s cyber insurance policy.⁴¹ Even though the firm had fully incorporated the NIST Cybersecurity Framework (CSF) into their risk management practices in the year since applying for the policy, the abbreviated questionnaire they received only asked if there had been any changes regarding the security and protection of their network in the last year, and if yes, whether they had experienced a security breach—giving them no option to indicate successful incorporation of the NIST CSF. As a result of increased revenue in the last year—and despite the robust cybersecurity controls she and her team had put in place—their premium increased by 12%. Insurers were, in effect, using firm revenue as their sole indicator of risk, and not considering other elements that could reduce that risk. The CEO testified, “When we asked whether or not using the CSF could be a factor, our broker wrote that ‘although they do not specifically inquire as to whether or not an insured is following the voluntary cyber security framework provided by NIST, they obviously take into consideration any preventative measures an insured implements when underwriting a risk.’”⁴² However, that consideration did not appear to be the case in practice.

38 Romanosky et al., “Content Analysis of Cyber Insurance Policies,” 14.

39 Woods and Moore, “Does Insurance Have a Future in Governing Cybersecurity?” 2.

40 Council of Insurance Agents & Brokers, “Cyber Market Watch Survey,” April 2015.

41 Wolff, *Cyberinsurance Policy*.

42 Ola Sage, “Examining the Evolving Cyber Insurance Marketplace,” written testimony before the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, March 19, 2015, <https://www.commerce.senate.gov/services/files/CFA8174A-E7F4-434A-9669-09282C0A8F1F>.

The Ransomware Era: New Forms of Security Assessment Emerge

By the late 2010s, businesses were contending with a new form of cyber risk: ransomware. Ransomware began as a small-scale form of computer-enabled crime, targeting individual computer systems for small amounts of fiat currency. Over the course of the late 2000s and into the 2010s, ransomware developed into a larger criminal enterprise, whereby gangs targeted businesses and organizations and demanded payments in digital currency. In contrast to the data breach notification era of cyber insurance, ransomware affects organizations of all sizes, not just large e-commerce entities storing significant amounts of consumer information. In addition to the risks of data exposure, companies facing a ransomware attack also encounter the risks of data deletion or distortion, extortion and ransom payment demands, and even physical damage—necessitating new forms of first- and third-party coverage.⁴³

Ransomware and extortion-based attacks pose an evolving threat of “triple extortion”: (1) an organization faces the immediate business continuity risks associated with its data being encrypted, seized, or altered, disrupting or halting operations; (2) an organization faces risks from sensitive data becoming exposed, leading to harms to its customers, possible litigation, and regulatory penalties (traditional data breach risks); and (3) an organization faces direct follow-on risks to customers, individuals, or associated parties in the form of distributed denial-of-service (DDoS) attacks, additional breaches or extortion of third party providers, or threats to life and property.⁴⁴

Of course, throughout this time period, organizations continued to face data breaches and other types of cyber risk, not just ransomware. However, the high-profile, widely-publicized nature of ransomware attacks contributed to increased demand for cyber insurance. From 2015 to 2020, the number of cyber insurers issuing policies in the U.S. marketplace rose from

43 Ransomware Task Force, “Combating Ransomware: A Comprehensive Framework for Action,” Institute for Security and Technology, April 2021, <https://securityandtechnology.org/ransomwaretaskforce/report/>; Woods and Wolff, “A History of Cyber Risk Transfer.” Ransomware can also result in physical damages, such as bricked physical systems, products that are spoiled due to manufacturing outages, or equipment damage. Often, these physical damages are covered under a specialized, supplementary policy. See for example: “Ransomware Gets Real: Bodily Injury and Property Damage,” case study, Coalition, Inc., last accessed February 2025, <https://www.coalitioninc.com/case-studies/manufacturing/cyber-insurance-reducing-ransomware-downtime>.

44 See, for example, “What is Triple Extortion Ransomware?” Checkpoint, last accessed February 2025, <https://www.checkpoint.com/cyber-hub/ransomware/what-is-triple-extortion-ransomware/>.

119 to 200.⁴⁵ Among insurers issuing standalone and package cyber policies, direct written premiums rose from \$2.38 billion in 2016 to \$4.07 billion in 2020.⁴⁶

Ransomware changed the profitability of the entire cyber insurance market. In 2015, before the explosion of ransomware incidents, loss ratios in the U.S. cyber insurance market for standalone and package policies averaged \$0.41 per dollar collected in premiums.⁴⁷ However, by 2020, due in part to increased losses from ransomware attacks, U.S. cyber insurers paid out claims at an average ratio of \$0.669 for every dollar collected in premiums for standalone and package policies—a ratio that varied from \$0.246 to \$1.14 per dollar of premiums collected.⁴⁸ In comparison, the overall U.S. property & casualty insurance market had an average loss ratio of \$0.70 for every dollar collected in premiums in 2020.⁴⁹ Even though the cyber insurance loss ratios resemble those of the overall P&C market, the difference is the extreme fluctuation—whereas average P&C loss ratios fluctuated between \$0.67 and \$0.74 from 2012 to 2021, average cyber insurance loss ratios fluctuated between \$0.41 and \$0.669 from 2015 to 2020.⁵⁰ As a result of significant losses in 2019 and 2020, the market started to harden, leading to higher premiums, more coverage exclusions, and greater barriers to entry for insureds.⁵¹

As customer demand for coverage increased and insurers no longer faced such stiff competition for customers and market share, insurers were able to deploy stricter measures to

-
- 45 Aon, “U.S. Cyber Market Update: 2019 U.S. Cyber Insurance Profits and Performance,” June 2020, <https://www.aon.com/reinsurance/getmedia/820de93d-6ff9-469b-af48-a6cf148cfaa6/202006-us-cyber-market-update.pdf.aspx>; Aon, “U.S. Cyber Market Update: 2021 U.S. Cyber Insurance Profits and Performance,” August 2022, <https://www.aon.com/reinsurance/getmedia/fa8eb0da-dec8-4205-bc46-12068d4b3d70/20220831-US-Cyber-Market-Update.pdf>.
- 46 For context, direct premiums in the U.S. admitted cyber insurance market made up only 0.38% of all U.S. property/casualty (P/C) direct written premiums in 2020, which totaled \$727.1 billion. In relative terms, however, this increase is significant: U.S. P/C direct written premiums only increased 19% from 2015 to 2020, whereas U.S. admitted cyber insurance direct written premiums increased by 412%. National Association of Insurance Commissioners, “Cybersecurity Insurance Market 2020,” October 20, 2021, https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf; National Association of Insurance Commissioners, “Property & Casualty Insurance Industry,” 2021, <https://content.naic.org/sites/default/files/industry-analysis-report-2020-property-casualty.pdf>; National Association of Insurance Commissioners, “U.S. Property & Casualty and Title Insurance Industries,” 2017, https://content.naic.org/sites/default/files/inline-files/topic_insurance_industry_snapshots_2016_prop_cas_title_ins_ind_report.pdf.
- 47 Aon, “U.S. Cyber Market Update: 2021 U.S. Cyber Insurance Profits and Performance,” August 2022, <https://www.aon.com/reinsurance/getmedia/fa8eb0da-dec8-4205-bc46-12068d4b3d70/20220831-US-Cyber-Market-Update.pdf>.
- 48 Aon, “U.S. Cyber Market Update: 2021 U.S. Cyber Insurance Profits and Performance”; National Association of Insurance Commissioners, “Cybersecurity Insurance Market 2020.”
- 49 National Association of Insurance Commissioners, “Property & Casualty Insurance Industry – 2021 Full Year Results,” 2022, <https://content.naic.org/sites/default/files/industry-analysis-report-2021-property-casualty.pdf>.
- 50 National Association of Insurance Commissioners, “Property & Casualty Insurance Industry,” 2021; Aon, “U.S. Cyber Market Update: 2021 U.S. Cyber Insurance Profits and Performance,” August 2022, <https://www.aon.com/reinsurance/getmedia/fa8eb0da-dec8-4205-bc46-12068d4b3d70/20220831-US-Cyber-Market-Update.pdf>.
- 51 Gareth Mott, Sarah Turner, Jason R.C. Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, Edward Cartwright, “Between a rock and a hard(ening) place: Cyber insurance in the ransomware era,” *Computers & Security* 128 (2023), <https://doi.org/10.1016/j.cose.2023.103162>.

assess risk, both for new policies and renewals.⁵² According to interviews conducted by one RUSI study, “insurers and businesses highlighted that [self] questionnaires have become much longer, more granular and more focused on assessing technical security controls since early 2021.”⁵³ Larger businesses in particular faced higher levels of scrutiny; as one chief risk officer at a large company describes it, they were faced with “very specific [questions]...the sort of questions you don’t want to be asked if you’re a big company.”⁵⁴ Security assessments for large corporations, according to one interview, could even involve site visits, interviews, and hardware examinations—the kinds of hands-on investigations not seen since the earliest days of the cyber insurance industry.⁵⁵

For SMEs, however, the levels of assessment did not always mirror those of large companies. One report found that SMEs might fill out a form with as few as four questions in order to secure coverage.⁵⁶ Asking a smaller entity to fill out a burdensome questionnaire could deter them from seeking out insurance altogether. Insurers who wanted to attract SMEs as policyholders, whether in an effort to diversify their risk portfolio or increase their market share, had to weigh the benefit of bringing them on as insureds with the potential downside of not fully understanding their level of cyber risk. Despite this lower bar to entry, as of 2024, only 10% of SMEs with annual revenues of under \$100 million carried cyber insurance—a stark contrast to the approximately 80% of companies bringing in annual revenues of over \$10 billion that held specific cyber coverage.⁵⁷

With new technology comes new ways to evaluate risk. Some insurers have incorporated security scans into their assessments, either using in-house or third-party technology.⁵⁸ These security scans, when used in tandem with other methods of evaluating risk, can be particularly useful as one data point for organizations employing well-known, commercially available products, particularly SMEs. For example, AWS runs the Cyber Insurance Competency Partner program, working with insurers to “streamline the process for AWS customers to get a quote for the cyber insurance coverage they need within 2 business days.”⁵⁹ In 2021, Google Cloud launched the Risk Protection Program, which provides all Google Cloud customers with a

52 Michael Rossi, “An Abbreviated History of Risk Management,” blog, March 2024, <https://www.korurm.com/blog/an-abbreviated-history-of-cyber-insurance---the-first-25-years>.

53 Jamie MacColl et al., “Cyber Insurance and the Ransomware Challenge.”

54 Jamie MacColl et al., “Cyber Insurance and the Ransomware Challenge.”

55 Jamie MacColl, Jason R C Nurse, and James Sullivan, “Cyber Insurance and the Cyber Security Challenge,” Royal United Services Institute for Defence and Security Studies, June 2021, <https://static.rusi.org/247-op-cyber-insurance-v2.pdf>.

56 MacColl et al., “Cyber Insurance and the Cyber Security Challenge.”

57 “Reality check on the future of the cyber insurance market,” SwissRe.

58 “Reality check on the future of the cyber insurance market,” SwissRe; Shauhin Talesh and Bryan Cunningham, “The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence’s Impact on Cybersecurity and Privacy,” *Utah Law Review* 2021, no. 5 (December 2021), <https://doi.org/10.26054/0d-9y6k-1t55>.

59 “AWS Cyber Insurance Competency Partners,” AWS, last accessed February 2025, <https://aws.amazon.com/partners/cyber-insurance-partner-solutions/>; “Search Results for Cyber Insurance Partners,” AWS, last accessed February 2025, <https://partners.amazonaws.com/search/partners?facets=Use%20Case%203A%20Cyber%20Insurance>.

tool that “maps [their] cloud configurations against industry standard CIS Benchmarks.”⁶⁰ The report can then be shared with partner insurers “directly from the UI,” who then provide access to enhanced “cyber insurance policies designed exclusively for Google Cloud customers.”⁶¹

Still others look to third-party products to assess the security posture of an organization and to ease the underwriting process. For example, SecurityScorecard partners with insurers to “improve the insurability of all organizations” by streamlining applications and optimizing pricing and coverage.⁶² Another example is Bitsight, which aims to help underwriters get “transparency into an applicant’s cyber risk.”⁶³ These scores can be a helpful starting point for a conversation about an organization’s level of risk.

For some prospective insureds, these scans can result in unreliable, inaccurate assessments of their cybersecurity posture. A 2021 study that interviewed 60 participants in cyber insurance highlighted potential problems with this assessment approach: companies may be outsourcing their information to third party or even fourth party vendors, or might be intentionally leaving honeypots to capture bad actors—situations that, without added context, might result in false positives or false negatives.⁶⁴ A decoy deliberately placed to capture bad actors might falsely indicate that a company is cyber insecure, when in reality the company is using the honeypot to distract actors from real targets or engage in reconnaissance efforts.⁶⁵ Likewise, if a company outsources its assets or security to external vendors that are not employing secure practices, a security scan of only the company’s internal security posture may indicate that they are cyber secure when in reality they face supply chain risks.⁶⁶

Cyber insurance can possibly play a larger role in overall cyber resilience, not only by assessing the security status of a business at the time of underwriting, but also through additional mechanisms outside of policy issuance and renewal. The following sections explore the options for pursuing security as a requirement and as an incentive, investigate the current state of the market, and examine barriers to further incentivizing cyber resilience from the outset through the specific case of bundling.

60 Phil Venables and Sunil Potti, “Announcing the Risk Protection Program: Moving from shared responsibility to shared fate,” Google Cloud, March 2, 2021, <https://cloud.google.com/blog/products/identity-security/google-cloud-risk-protection-program-now-in-preview>.

61 “Risk Protection Program,” Google Cloud, last accessed April 2025, <https://cloud.google.com/security/products/risk-protection-program>.

62 “Cyber Insurability Alliance,” SecurityScorecard, last accessed February 2025, <https://insurance.securityscorecard.com/cyber-insurability-alliance/>.

63 “Bitsight for Cyber Insurance,” Bitsight, last accessed February 2025, <https://www.bitsight.com/products/bitsight-for-cyber-insurance>.

64 Talesh and Cunningham, “The Technologization of Insurance.”

65 Narendran Vaideeswaran, “Honeypots in Cybersecurity Explained,” CrowdStrike, January 16, 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/>.

66 Kaitlyn Graham, “What is Fourth-Party Risk vs. Third-Party Risk?” Bitsight, April 11, 2024, <https://www.bitsight.com/blog/what-third-party-vs-fourth-party-risk-and-how-manage-both>.

Examining the Strategic Potential of Cyber Insurers

Cyber insurance is a growing but relatively underdeveloped market. While the current ecosystem has many limitations, cyber insurance carriers may be well positioned as third parties to help organizations improve their cybersecurity posture for three reasons:

1. A common goal:

In the long term, insurers and policyholders may share a common goal: preventing cyber incidents. Businesses want to avoid costly disruptions, reputational damage, and financial losses, while insurers seek to minimize claims that affect profitability and market sustainability. In the short term, these goals may be at odds, and can even push both insurers and insureds to pursue low-cost, low-impact fixes. Yet over time, insurers and insureds both benefit from investments in cybersecurity that reduce the risk of incident to policyholders, and lower the costs of one should it occur. If incentives can be properly aligned in the marketplace, insurers may have a vested interest in helping policyholders improve cybersecurity by allocating limited resources efficiently. Through increased data sharing and more robust partnerships, insurers may even help guide insureds toward security solutions that best fit their risk profile and needs.

2. Addressing cyber risk with applicable security controls:

Policyholders—especially small- and medium-sized businesses—often struggle to understand the extent and potential consequences of their own cyber risk, frequently believing their organization is too small to be a lucrative target, despite growing evidence to the contrary.⁶⁷ While recommendations for cybersecurity practices abound, few are grounded in empirical study.⁶⁸ The landscape for SMEs is therefore littered with different guidance that can overwhelm small or under-resourced security teams.⁶⁹ Insurers are some of the only actors

67 See, for example: Mika Pangilinan, “Small businesses underestimating their vulnerability to cyber risks – survey,” Insurance Business Magazine, September 28, 2023, <https://www.insurancebusinessmag.com/ca/news/cyber/small-businesses-underestimating-their-vulnerability-to-cyber-risks--survey-461246.aspx>; Colin Hanks, “Small Business Ransomware: What You Need to Know,” Veeam, January 24, 2024, <https://www.veeam.com/blog/small-business-ransomware.html>.

68 Stewart Scott, “Counting the Costs in Cybersecurity,” *Lawfare*, October 9, 2024, <https://www.lawfaremedia.org/article/counting-the-costs-in-cybersecurity>; Paul Rosenzweig, “Preliminary Observations on the Utility of Measuring Cybersecurity,” *Lawfare*, August 6, 2019, <https://www.lawfaremedia.org/article/preliminary-observations-utility-measuring-cybersecurity>.

69 The Small Business Administration lists nine different government guides for small businesses as part of its own guide, each with a separate set of recommendations. U.S. Small Business Administration, “Strengthen your cybersecurity,” last updated July 2, 2024,

in the broader cyber ecosystem with access to data that tie security controls to security outcomes, namely, cyber insurance claims. Using these data, insurers can look at the efficacy of management security controls,⁷⁰ which are often assessed at underwriting. They may then be able to make recommendations to their policyholders about which controls to prioritize that are based not on expert opinion, but on empirical data.⁷¹

Cyber insurers are a particularly attractive source of these insights not only because of their unique data sets, but also because of the competition inherent to their risk pricing. Insurers with novel understandings of control sets should be able to price premiums accordingly. If they are correct, they profit while simultaneously driving their insureds to more secure cybersecurity paradigms. And, if they are wrong, they suffer in the market, even while their customers are protected by their ability to file claims.

3. Deeper risk insights:

Beyond management-based security controls, insurers also have the potential to unlock deeper insights today, especially when security postures are often self-reported. By integrating real-time data from security providers, insurers increasingly have the option to carry out continual compliance, which assesses the implementation of a company's cybersecurity policies, not just the fact that they exist.⁷² Insurers can derive insights from these additional data about security controls that are easier to implement, and drive their policyholders to more practical solutions. Continuous data streams also allow an insurer to check in with a policyholder if they observe a deviation from the baseline, potentially pre-empting a breach.⁷³

The market, however, has yet to reflect this idealized state. As explored in the previous section, early, experimental cyber insurance policies involved lengthy, in-depth security assessments that attempted to gauge a broad range of cyber risks faced by a potential insured. During this period, insurers also capitalized on partnerships with external vendors to try to better assess a new and developing market. However, following the introduction of new data breach notification laws and the subsequent shift to a soft market in the 2000s and early

<https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity>.

- 70 Healey discusses “management-based regulations”; however, as insurers are similarly positioned to government regulators in that they are outside entities levying requirements, the analysis remains useful in understanding what kinds of controls are considered in underwriting. Healey defines management-based regulations as “mandat[ing] general planning and management practices.” Jason Healey, “Which Cyber Regulations Fit Which Sectors?” *Lawfare*, November 20, 2023, <https://www.lawfaremedia.org/article/which-cyber-regulations-fit-which-sectors>.
- 71 “Using Data to Prioritize Cybersecurity Investments,” Marsh McLennan, GuyCarpenter, Mercer, OliverWyman, 2023, https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Using_data_to_prioritize_cybersecurity_investments_report.pdf.
- 72 Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, and Kevin Stine, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” NIST, September 2011, <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf>.
- 73 Ryan Gregory, “How Proactive Mitigation Helps SMBs Reduce Cyber Exposure,” Coalition, August 27, 2024, <https://www.coalitioninc.com/blog/proactive-risk-mitigation>.

2010s, cyber insurers relied more heavily on self-questionnaires, often focusing more narrowly on data breach risks targeted by the new regulations. Insurance policies have to date largely dealt with managing fallout after an incident, rather than on helping businesses to improve their security before an incident occurs. While insurers have the strategic potential to help organizations navigate the crowded and opaque security services market, given (1) a shared long-term goal, (2) their possible improved ability to address cyber risk with applicable security controls, and (3) their potential to access deeper risk insights, this is not yet the de facto operating reality of the current market.

Towards Cybersecurity and Cyber Resilience: Security as a Requirement and as a Benefit

Over the course of the last two decades, the cyber insurance market has oscillated between hard and soft markets, leading to some shifts in the way that underwriters and brokers categorize and measure cyber risk. Neither end of the spectrum has led to optimal results: cyber insurance has yet to become a robust tool to help insureds implement cyber hygiene and security standards to defend against an incident, or to make them more resilient in the event that one should occur.

How do we move towards a world in which cyber insurance can help businesses adopt better security measures from the outset, and in turn achieve overall cyber resilience? In theory, this shift could come about in two ways:

- 1. Cyber insurers could *require* businesses to adopt better security by declining to cover them; reducing their coverage either by providing hard limits or lowering coverage per dollar of premium; or denying claims.**
- 2. Cyber insurers could *incentivize* businesses to adopt better security, either through premium reductions at the time of underwriting or through rebates over the course of their policy.**

Brandishing “Sticks”: Options for pursuing security as a requirement

In order to carry out this role as risk mitigator and manager, insurers can approach security as a requirement, brandishing a “stick” to motivate their insureds to become more secure. The efficacy of requirements, however, is limited by the market dynamics at play. In a soft market, competition will drive premiums down, making it harder for insurers with more onerous requirements to compete. Importantly, pursuing security as a requirement raises the potential of conflict between insurers and insureds, rather than encouraging alignment around the shared goal of cyber resilience.

Pursuing security by requirement can involve a number of scenarios. First, an insurer could outright decline to issue a policy to a business who fails to comply with specific security baselines that are baked into the policy from the outset, rather than charging them the actuarially-approved price of the risk on their premiums. Even in a hard market with high demand, declination of coverage is unpopular. Especially given continued competition in the cyber insurance marketplace, cyber insurers are likely to prioritize gaining market share and increasing the amount of policyholders they have over enforcing security standards by declining to insure a business. This kind of soft market breeds “race to the bottom” dynamics for security standards.

Rather than decline to cover a business entirely, an insurer could reduce coverage for those businesses who do not comply with policy requirements that enforce security standards, rather than charging them for the actuarially-appropriate price of the risk on their premiums. For example, one insurer introduced a “45-day grace period” for policyholders to patch known software vulnerabilities; after the grace period is over, the insured “takes on progressively more of the risk if the vulnerability is not patched at the 46-, 90-, 180-, and 365-day points.”⁷⁴ However, as Daniel Woods highlights, this requirements-centered approach necessitates that insurers build an explicit reference to those controls or actions that lead to better security into the policy from the outset.⁷⁵ Such contractual language could be inconsistent with technical cybersecurity realities. In some cases, a patch may not be possible, leading policyholders to seek alternate mitigations like placing assets behind a firewall. The language may also be

74 “Chubb Addresses Growing Cyber Risks with a Flexible and Sustainable Approach,” Chubb, October 13, 2021, https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/cyber-enterprise-risk-management-cyber-erm/documents/pdf/2021-10.13_v3_17-01-0295_Widespread_Events_Endorsements.pdf.

75 Daniel Woods, “A Turning Point for Cyber Insurance,” *Communications of the ACM* 66, 3 (March 2023), <https://doi.org/10.1145/3545795>.

impractical to enforce, particularly when there is insufficient evidence to demonstrate that the root cause of a claim is a specific unpatched vulnerability.⁷⁶

Lastly, cyber insurers could pursue security as a requirement by denying claims if security procedures are not followed. All insurers can contest, litigate, and deny claims as a basic tool to enforce the terms of the insurance policy. In theory, denying claims can ensure that the market avoids moral hazard—the possibility that an insured, once covered by insurance, is not properly incentivized to avoid risk.⁷⁷ However, the limited data we have indicates that claims denial may not be common. For example, in a 2022 survey of 5,600 IT professionals worldwide, Sophos finds that cyber insurers paid out some or all of the costs in 98% of incidents where the victim had cyber insurance that covered ransomware.⁷⁸ The perception that claims denial is widespread may also be due, in part, to media reporting. In a 2023 analysis sampling information from 101 media articles about cyber insurance disputes, the majority focused on hypothetical disputes. In cases of reporting on actual disputes, only 17% related to standalone cyber insurance policies.⁷⁹ However, researchers need more data to truly assess the level of full and partial claims denial being carried out by the cyber insurance market.

Denying claims has the potential to invite lawsuits or other legal disputes between insurers and policyholders. For example, a 2015 lawsuit filed by an insurer against a health system over a 2013 data breach alleged that the hospital network had failed to “continuously implement the procedures and risk controls identified in the Insured’s application,” including secure configurations, regular security patching, and due diligence over its third party vendors.⁸⁰ The suit, which was ultimately dismissed because the insurer did not pursue alternative dispute resolution, demonstrates the potential costs of pursuing security as a requirement, including litigation. Another lawsuit filed in 2022 between an insurer and a manufacturing company alleged that the manufacturing company had misrepresented its level of multi-factor authentication, only securing its firewall but not its server and other digital assets.⁸¹ The insurer sought not only to deny the claim, but also rescind coverage and void the insurance

76 Zoë Brammer, “Putting the Blueprint for Ransomware Defense to the Test,” Institute for Security and Technology, August 28, 2023, <https://securityandtechnology.org/blog/putting-the-blueprint-for-ransomware-defense-to-the-test/>.

77 Ben-Shahar and Logue, “Outsourcing Regulation: How Insurance Reduces Moral Hazard.”

78 Sophos, “The State of Ransomware 2022,” April 2022, <https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf>.

79 Daniel W. Woods, “Don’t Mention the War: Bias in Reporting on Cyber Insurance Disputes,” *Cyber Economics*, no. 1 (August 2023), <https://cyber-economics.com/2023/08/29/thoughtleadership-piece-01/>.

80 John Buchanan, Ben Duke, and Scott Levitt, “Cyber Insurer Seeks to Void Data Breach Coverage Because of Purported Misstatements in Policy Application,” *Inside Privacy*, Covington, June 16, 2016, <https://www.insideprivacy.com/data-security/cybersecurity/cyber-insurer-seeks-to-void-data-breach-coverage-because-of-purported-misstatements-in-policy-application/>.

81 Jennifer Bentley, “Using Multi-Factor Authentication as a Prerequisite to Cyber Liability Coverage,” *JDSupra*, Farella Braun + Martel LLP, August 12, 2022, <https://www.jdsupra.com/legalnews/using-multi-factor-authentication-as-a-2167531/>.

contract between the two.⁸² The case ended in the rescission of the manufacturer’s policy.⁸³ As these two cases illustrate, pursuing security as a requirement through claims denial can be an option for insurers willing to spend the time and effort in court, but does not come with a guaranteed outcome.

Insurance regulation mandates that scenarios in which an insurer might decline coverage, reduce coverage, or deny claims must be written into the policy itself in order to be enforceable, either at the time of underwriting or renewal.⁸⁴ This process does not incentivize preemptive investment in security: the insured either pays for a higher premium that covers its additional risks, the insurer reduces coverage, or some combination thereof. Outside of the underwriting process, both insurers and insureds are more likely to be motivated to reduce costs after an incident occurs rather than partner to improve security before an incident occurs when it cannot be reflected in the existing policy. In other words, the policyholder does not stand to gain—at least vis-à-vis its insurance policy—by improving its security between the purchasing of a policy and the renewal.

More broadly, the practices of declining or reducing coverage or denying claims do not help align the shared goals of insurers and insureds to mitigate cyber risk. If cyber insurance is to be a tool to improve the security posture of the entire ecosystem, it has to be used. When insurers deem a risk to be uninsurable, rather than working with their policyholders to mitigate risk, we do not realize the benefits outlined by Schneier over two decades ago.

Offering “Carrots”: Options for pursuing security as a benefit

Insurers could also pursue security as a benefit, using “carrots” to incentivize their insureds to become more secure. Incentives, importantly, can be effective in both hard and soft markets. Even in a soft market, when premiums drop and insurers cannot easily hold insureds to strict standards in order to qualify for a policy, incentives can still be a valuable mechanism through which to mitigate risk and manage loss. Insurers pursuing security as a benefit could provide incentives in two scenarios: at the time of underwriting or over the course of the policy.

82 Stephen Lawton, “Cyber Insurers Clamp Down on Clients’ Self-Attestation of Security Controls,” *DarkReading*, September 21, 2022, <https://www.darkreading.com/cyber-risk/cyber-insurers-clamp-down-on-clients-self-attestation-of-security-controls>.

83 Richard Bortnick and Jonathan Meer, “Practical Applications of *Travelers v. ICS* for Cyber Insurance Brokers, Carriers, and Policyholders: Emerging Trends and Predictions,” *The National Law Review*, Wilson Elser Moskowitz Edelman & Dicker LLP, February 8, 2023, <https://natlawreview.com/article/practical-implications-travelers-v-ics-cyber-insurance-brokers-carriers-and>.

84 Nancy Germond, “Why Do Insurance Policies Have Exclusions?” Independent Insurance Agents & Brokers of America, January 5, 2024, <https://www.independentagent.com/vu/Agency-Management/Miscellaneous/GermondWhyPolicyExclusionsExist.aspx>.

A Note on Terminology: Anti-inducement, anti-rebating, and anti-bundling

Under state insurance laws, inducement, rebating, and bundling are terms used in the context of unfair trade practice and consumer protection regulations. These terms are often used imprecisely in the literature and in practice, but refer to related yet distinct concepts—each with different regulatory implications under state law. **Anti-inducement** rules prohibit insurers and agents from offering unapproved incentives like free gifts, premium discounts, or value-added services to persuade an entity to buy a policy when such incentives are not specified in the contract.

Anti-rebating rules refer to a more narrow subset of anti-inducement rules. Rebating generally refers to an insurer or broker giving back part of their commission or other perk to induce a customer to purchase a policy, when that rebate isn't explicitly reflected in the insurance policy.

Bundling refers to the combining of an insurance product with a non-insurance, value-added product or service that helps to mitigate or manage loss.⁸⁵ Anti-bundling rules restrict the types of services that may be provided to customers without being explicitly written in the policy itself, requiring for example that they provide loss mitigation or loss control; reduce claim costs; or provide education about liability risks.⁸⁶ Bundling is typically permissible provided bundles are structured within approved rating and underwriting guidelines, unlike inducements and rebates which may be more broadly restricted under some state laws.

For the purposes of this piece, we use the word bundling as a catch-all to refer to a circumstance in which a cyber insurer presents an organization with one or more optional non-insurance security products or services that they can purchase at additional cost with their cyber insurance policy. The combination of the non-insurance security product or service with insurance results in a reduced rate on the security product or service or a rebate on the policy premium that reflects the risk reduction anticipated from implementing the optional product or service—whether those services are purchased through a third party or insurer affiliate. Unlike co-marketing partnerships, which result in a reduced premium at the time of underwriting or renewal, bundling has the potential to reduce the amount that an insured pays not just at the time of underwriting or renewal, but over the course of the policy.

Non-insurance risk reduction features that come standard with every policy—provided at no additional cost and made mandatory—are not typically treated as bundles in the regulatory context. We will refer to these as embedded policy features, and exclude them from our definition of bundling in this report. For example, a cyber insurance policy that includes security scans or customized policyholder vulnerability alerts as a standard policyholder benefit would be considered an embedded policy feature under a cyber insurance policy.

Currently, the regulatory landscape for bundling is complex, and rules differ between states. In many states, bundling may be allowed if the specifics of the services provided or rate reductions offered are outlined in the insurance policies at the time of issuance or renewal. Due to variation in state law and perceptions of bundling, insurers often lack clarity regarding what they can do to incentivize better security through bundling, outside of what is formally or explicitly written into a policy.⁸⁷

85 National Association of Insurance Commissioners, “Bundling,” last updated February 10, 2025, <https://content.naic.org/insurance-topics/bundling>.

86 National Association of Insurance Commissioners, “Unfair Trade Practices Act,” Model Law 880-1, Spring 2024, <https://content.naic.org/sites/default/files/model-law-880.pdf>.

87 Ann Young Black, “The Gift of Giving: States Move to Amend Their Anti-Rebating Laws,” *JDSupra*, Carlton Fields, May 6, 2021, <https://www.jdsupra.com/legalnews/the-gift-of-giving-states-move-to-amend-6318086/>; Jamie Parson, David Marlett, and Stuart Powell, “Time to Dust Off the Anti-Rebate Laws,” *Journal of Insurance Regulation* 37, no. 7 (2017), <https://content.naic.org/sites/default/files/jir-za-36-07-el-dust-off-anti-rebate.pdf>.

First, insurers could offer up-front reductions on policy premiums or unlock higher policy limits during the underwriting process to reward better security. Up-front premium reductions or higher policy limits could be associated with specific security controls or practices that a business demonstrates it has put in place at the time of underwriting. For example, an insurer might offer a higher policy limit or a discount on a premium for a business that can demonstrate its adherence to common cybersecurity frameworks such as the CISA Cybersecurity Performance Goals, NIST 800-171 on Protecting Controlled Unclassified Information, the Center for Internet Security's Critical Security Controls Implementation Group 1, or another sector-specific set of controls.⁸⁸ Such discounts for adherence to cybersecurity standards or frameworks were a common feature of the early days of cyber insurance, as illustrated in [A Brief History of Cyber Insurance](#).

However, since these rate reductions must be written directly into the policy at issuance or renewal, this form of up-front incentive does not consider the security posture of a business over the course of the policy. An organization that has secured a policy may be less incentivized to make continual updates as new cyber threats emerge or as risks to their business change. In addition, cybersecurity itself is a constantly moving target. Threat actors evolve and adapt, finding new ways to orchestrate attacks. Most experts agree that many relatively low-cost cyber hygiene practices still need to be implemented across companies.⁸⁹ Particularly for SMEs, incentivizing the adoption of a basic set of controls that work to prevent the most frequent attack vectors could be an effective way to bolster cyber resilience, but this approach is not comprehensive.

Rather than selecting a specific framework or standard, insurers could instead incentivize security by partnering with security firms or other providers at the time of underwriting to offer a reduced premium rate or higher policy limits for insureds that use a particular security product or service, called a co-marketing partnership. An insurance company could also offer a survey of products within a certain category of service, such as managed detection and response (MDR). These co-marketing partnerships can ease the process of underwriting, making it simpler for a business to demonstrate their security posture and qualify for coverage. For example, through Cloudflare's Cyber Risk Partnership program, prospective insureds can "qualify for better coverage and premiums from [Cloudflare's] insurance partners" by demonstrating their use of Cloudflare's protection.⁹⁰ Likewise, prospective insureds who use

88 Ron Ross and Victoria Pillitteri, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST NIST SP 800-171 Rev. 3, May 2024, <https://csrc.nist.gov/pubs/sp/800/171/r3/final>; "CIS Critical Security Controls Implementation Group 1," Center for Internet Security, last accessed February 2025, <https://www.cisecurity.org/controls/implementation-groups/ig1>; CISA, "Cross-Sector Cybersecurity Performance Goals," last accessed February 2025, <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>.

89 Center for Internet Security, "Essential Cyber Hygiene: Making Cyber Defense Cost Effective," August 2023, <https://www.cisecurity.org/insights/blog/essential-cyber-hygiene-making-cyber-defense-cost-effective>.

90 Cloudflare, "Cyber Risk Partnerships," last accessed April 2025, <https://www.cloudflare.com/partners/cyber-risk/>.

the AWS Security Hub as “a simplified method of sharing your AWS security posture” can get a quote within 2 business days and “can offer valuable insights as to how the customer can level up their security posture even higher, thereby further reducing the customer’s business risk while unlocking higher coverage limits or reducing the cost on premiums for the customer.”⁹¹ In another example, At-Bay offers a 15% discount on premiums when insureds using Microsoft 365 implement MFA for all network and email access, and Microsoft Defender for Office 365.⁹² These partnerships, especially for SMEs who tend to use commoditized, off-the-shelf solutions more frequently than large enterprises, could make acquiring coverage easier and cheaper.⁹³

Another option for offering security as a benefit could be to combine services that boost security together with a cyber insurance policy, either as an option at an additional cost (bundling), or at no additional cost as a standard policyholder benefit (embedded policy feature). By combining insurance with additional products or services, insurance providers can manage an insured’s risk, reduce future claims, and even gather more information to support future risk mitigation tactics. In the cyber insurance context, a firm might combine insurance with vulnerability scanning services, attack surface monitoring, threat intelligence reports, and incident response planning. Firms may also bundle, at an additional cost, intrusion detection and prevention services, firewalls, and other security management products and services.

Digital Forensics and Incident Response (DFIR): A Comparison

To understand how bundling works in practice, it is useful to compare it to the role of digital forensics and incident response (DFIR) in post-breach risk mitigation and loss management. Post-breach incident response is offered by the large majority of insurers as an additive service that helps to mitigate or reduce losses.⁹⁴ This is an example of a value-added service, but not an example of bundling. Unlike in the case of bundling, insurers incorporate DFIR into the insurance policy from the outset, neither requiring insureds to pay out of pocket for any additional services nor sign agreements with another provider. Should an incident occur, insurers instruct their policyholders to contact an incident hotline and choose from a “panel” of incident response firms to help them as they respond to the incident.

This set-up has many parallels to paneling in health insurance, when an individual with personal health insurance chooses from an in-network panel of doctors who have pre-negotiated rates with an insurer and often come at a discounted rate vis-à-vis out-of-network doctors. In the case of cyber insurance, the insured chooses from an in-network panel of incident response firms with

91 AWS, “AWS Cyber Insurance Competency Partners: Cyber insurance simplified,” last accessed April 2025, <https://aws.amazon.com/partners/cyber-insurance-partner-solutions/>.

92 At-Bay, “Premium Savings for Smart Security Choices,” last accessed February 2025, <https://www.at-bay.com/microsoft/>.

93 Stefano da Empoli and Giusy Massaro, “SME Adoption of Digital Technologies: A Transatlantic View,” Institute for Competitiveness, October 2021, https://www.transatlantic.org/wp-content/uploads/2022/01/11-03-2021-SME-digitalization_SdE-GM-final.pdf; Narges Kasiri, Cara Cirino, and Cameron Narimanian, “The Patterns of Business Analytics Adoption in US SMEs: A Qualitative Approach,” *Small Business Institute Journal* 20, no 1 (2024), <https://sbij.scholasticahq.com/article/115381-the-patterns-of-business-analytics-adoption-in-us-smes-a-qualitative-approach>.

94 Jamie MacColl et al, “Cyber Insurance and the Ransomware Challenge”; Daniel Woods, Rainer Böhme, Josephine Wolff, and Daniel Schwarcz, “Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys,” *Proceedings of the 32nd USENIX Conference on Security Symposium* no. 127, August 2023, <https://dl.acm.org/doi/10.5555/3620237.3620364>.

whom insurers have already negotiated the rates (typically 70% of market value) who are available to help. If an insured wants to go out of network, or off-panel, they must specify that preference at the time of policy issuance. Since insurers may only reimburse at the rate pre-negotiated with their panel, going off panel would require an insured to pay the difference.⁹⁵ If panel members do not meet expectations, insurers can remove them, in effect allowing insurers to impose negative consequences on poor performance.⁹⁶

When putting DFIR panels together, insurers vet potential firms, pre-negotiate a price that the insurer will pay for their services (often at a reduced rate to the insurance company), connect firms with insureds, evaluate their performance, and even sometimes remove underperforming firms from their panels. Likewise, in bundling insurance with another product or service, insurers could vet security providers to offer to their customers, pre-negotiate a price for the product or service and even opt to provide a discounted rate, connect them with their insureds, and then evaluate their performance over the long term through claims data.

DFIR paneling—as with many dynamics in the realm of cyber insurance—is a newer practice and thus has generated limited data (especially when compared to paneling in medical insurance, for example). The practice has received a mixed reception. Policymakers and cybersecurity professionals have publicly speculated that cyber insurance may actually incentivize ransom payments—or even make organizations more compelling targets to attackers.⁹⁷ Researchers have investigated this phenomenon, but thus far the evidence is largely anecdotal: as a RUSI study on cyber insurance and ransomware puts it, “cyber insurance’s influence on victim decision-making is considerably more nuanced than the public debate has captured so far. While there is evidence that cyber insurance policies exfiltrated during attacks are used as leverage in negotiations and to set higher ransom demands, the conclusion that ransomware operators are deliberately targeting organisations with insurance has been overstated.”⁹⁸

According to a 2023 survey of participants in IR, some also worried that these panels could lower the quality of incident response overall. Other respondents maintained that providing panels could be highly beneficial for ease of access. As one survey participant explained, “having a panel of companies that all work together with pre-negotiated contracts and pre-negotiated rates resolves the issues of compatibility and contract negotiation during a crisis.”⁹⁹ Panels may also expedite incident response for SMEs who may not have the bandwidth or experience to know which services are available from which providers, much less be able to adjudicate their relative quality.

Researchers need more data to explore the effectiveness of DFIR panels in responding to cyber incidents, assess any positive or negative externalities, and understand how post-breach interventions ultimately affect cyber insureds’ levels of resilience.

Because DFIR services are available to all insureds under a given policy, and because these are services offered in the aftermath of an incident, they do not explicitly create a “carrot” to incentivize insureds to adopt better security. Bundling value-added cybersecurity products and services with insurance that can help insureds, like vulnerability scanning services and security management, has the potential to act as an incentive for insureds to boost their security prior to an incident.

95 Woods, Böhme, Wolff, and Schwarcz, “Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys.”

96 Daniel Woods and Rainer Böhme, “How Cyber Insurance Shapes Incident Response: A Mixed Methods Study,” *Proceedings of the 20th Annual Workshop on the Economics of Information Security*, June 29, 2021, <https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-woods.pdf>.

97 Anne Neuberger, “The Ransomware Battle is Shifting – So Should Our Response,” *The Financial Times*, October 4, 2024, <https://www.ft.com/content/3b172a2a-4be5-4ef4-87cb-7fdcdde2ad99>; Talion, “Ransomware Perceptions Report, 2021,” August 2021, https://talion.net/wp-content/uploads/2021/08/Talion-Report_final.pdf.

98 Jamie MacColl et al., “Cyber Insurance and the Ransomware Challenge.”

99 Woods, Böhme, Wolff, and Schwarcz, “Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys.”

Rather than providing the same service to all insureds and writing it explicitly into every insurance policy issued, bundling means that insurers could offer additional, non-insurance products and services that complement an insured's policy and risk profile at a reduced rate or accompanied by a rebate on the insurance premium. These services would not need to be explicitly tied to the insurance policy as written—instead, they could adapt over time as the insured's risk profile develops, and not just at the time of underwriting and renewal.

For example, after purchasing cyber insurance, an organization might decide that they want to invest in a cloud security product. Bundling would allow the organization's insurer to facilitate a discount on that product. Over the course of the insurance policy, the external cloud security service provider could generate real-time data for the insured on their level of risk and help them to resolve any issues before a breach occurs. Similarly, a firm could purchase an insurance policy and then decide to purchase Managed Detection and Response (MDR) a few months later, whereby the policy unlocks a discount on a specific service or set of services from pre-designated companies. Yet another example of bundling could involve the packaging of in-house security expertise with insurance, likewise unlocking a discount by pairing the two together. With more direct integration between the insurer and the security provider, there may be more opportunities for collaboration and for lowering risk profiles over time.

For example, insurer Chubb partners with security provider SentinelOne to provide endpoint protection and incident response to large insureds over the course of their policy. In articulating the incentives associated with this partnership, a Chubb press release stated, “The benefits for policyholders and their agents include providing potentially incentivized policy pricing subject to applicable insurance laws, streamlined policy renewals, and visibility and cyber threat protection through SentinelOne. Furthermore, subject to applicable insurance laws, these policyholders can also receive a discounted subscription to SentinelOne's solutions empowering them to keep their systems and data safe.”¹⁰⁰ As an example of an in-house security service offering, Coalition Inc. offers Coalition Control, a proprietary external scanning engine that leverages claims data and threat intelligence to assess a businesses' security posture at the time of underwriting and throughout the life of the policy. Coalition Control can also integrate with certain cloud service providers like Amazon, Google, and Microsoft to help policyholders actively manage and improve their cybersecurity posture.¹⁰¹ Another example of bundled security offerings is Beazley Security, an in-house cybersecurity firm within the insurer Beazley, which provides risk management services such as “Managed eXtended Detection and Response (MXDR)” and technical security to Beazley

100 “Chubb and SentinelOne Partner to Enhance Cyber Risk Management,” press release, September 27, 2023, <https://news.chubb.com/2023-09-27-Chubb-and-SentinelOne-R-Partner-to-Enhance-Cyber-Risk-Management>.

101 “Coalition Control,” Coalition, Inc., last accessed February 2025, <https://www.coalitioninc.com/control>.

insureds. Beazley also partners with external vendors like Charles River Associates and SecurityScorecard.¹⁰²

Whereas traditional insurance policies can only provide discounts at the time of underwriting or during the renewal process, a bundled security and insurance package might incorporate discounts or rebates into the security service, rewarding best practices or adoption of new cybersecurity frameworks over time. Bundling could be a solution tailored to the needs and risk profile of that company. If the underwriting process finds that a company struggles to implement tiered access controls and permissions, for example, the bundled security offering could step in to help. SMEs, in particular, could stand to benefit from bundling: rather than having to “go it alone” implementing cybersecurity, they could look to security products and services to help them become more resilient at a more affordable price. By acquiring these bundled offerings, SMEs could also become better positioned to qualify for more robust insurance policies, ultimately transferring risk and improving broader ecosystem cybersecurity.

Table 1: Partnerships between insurers and security providers

	Co-marketing partnerships	Bundled security services	Embedded policy features
Purpose	Simplify access to coverage. Help prospective insureds qualify for coverage, and help insurers better collect data about their levels of cyber risk through the underwriting process	Help an insured mitigate or manage loss and reduce their risk	Help an insured mitigate or manage loss and reduce their risk
Cost	Additional cost to the insured	Additional cost to the insured	No additional cost to the insured
How is the benefit realized?	Rate reduction on premiums for policyholders or increase in the amount of coverage available	Rate reduction for the security product or service or a rebate on the policy premium that reflects the risk reduction anticipated from implementing the product or service	No rate reduction
When is the benefit realized?	At the time of underwriting, as part of the underwriting process	At any point over the course of the policy, not part of the underwriting process	At any point over the course of the policy, part of the underwriting process

102 Rich Freeman, “Cyber Insurers are Cutting Out the MSP Middleman,” *Channelholc*, August 23, 2024, <https://www.channelholc.news/p/cyber-insurers-are-cutting-out-the>; “Discounted Prevention Services,” Beazley, last accessed February 2025, <https://www.beazley.com/en-US/cyber-customer-centre/cyber-risk-management-tools/cyber-prevention-services/>; “Fortifying Cyber Defences with Managed eXtended Detection and Response (MXDR),” Beazley, last accessed February 2025, <https://www.beazley.com/en-US/cyber-services-snapshot/fortifying-cyber-defences-with-managed-extended-detection-and-response-mxdr/>.

Examples

Not a comprehensive list, meant to illustrate what each of these incentives looks like in practice

Co-marketing partnerships

Cloudflare's Cyber Risk Partnership program:

Prospective insureds can “qualify for better coverage and premiums from [Cloudflare’s] insurance partners” by demonstrating their use of Cloudflare’s protection.¹⁰³

AWS Partner Program:

In addition to easing the underwriting process, insureds can “unlock higher coverage limits or reduce the cost on premiums” when they use the AWS Security Hub to reduce their risk.¹⁰⁴

AIG CyberMatics:

“Risk managers may benefit from more tailored and improved policy terms and conditions through AIG’s assessment of verified underwriting information.” Current partners include CrowdStrike, Darktrace, TechGuard Security, and Threater.¹⁰⁵

At-Bay and Microsoft:

Prospective insureds can unlock a 15% rate reduction on their premiums when using Microsoft 365 if they implement MFA for all network and email access and Microsoft Defender for Office 365.¹⁰⁶

Bundled security services

Chubb and SentinelOne:

Through a partnership with SentinelOne, insureds can access cyber threat protection through SentinelOne. “The benefits for policyholders and their agents include providing potentially incentivized policy pricing subject to applicable insurance laws, streamlined policy renewals, and visibility and cyber threat protection through SentinelOne. Furthermore, subject to applicable insurance laws, these policyholders can also receive a discounted subscription to SentinelOne’s solutions empowering them to keep their systems and data safe.”¹⁰⁷

At-Bay: For a fee, insureds can access At-Bay Stance, “a unified security platform that can protect your endpoints, identity, email, and cloud environments from adversaries — all in concert with your insurance policy.”¹⁰⁸

Embedded policy features

Hiscox: At no additional cost, insureds can access Upfort Shield, which provides “software protections, live consultative services, and security training content, including phishing simulations.”¹⁰⁹

Chubb: Through a partnership with BitSight, insureds can access complimentary external vulnerability monitoring, which can help them to “monitor cyber risk as a daily measurement of [their] security performance via a platform that highlights both strengths and potential weaknesses — providing key metrics and giving [them] visibility into the security of [their] organization.”¹¹⁰

Starr: Through a partnership with Rapid7, insureds have the “opportunity to access a complimentary external network vulnerability scan of up to 50 IP addresses.”¹¹¹

103 Cloudflare, “Cyber Risk Partnerships,” last accessed April 2025, <https://www.cloudflare.com/partners/cyber-risk/>.

104 AWS, “AWS Cyber Insurance Competency Partners,” last accessed April 2025, <https://aws.amazon.com/partners/cyber-insurance-partner-solutions/>.

105 AIG, “CyberMatics®,” last accessed April 2025, <https://www.aig.com/home/risk-solutions/business/cyber/cybermatics>.

106 At-Bay, “Premium Savings for Smart Security Choices,” last accessed April 2025, <https://www.at-bay.com/microsoft/>.

107 Chubb, “Chubb and SentinelOne® Partner to Enhance Cyber Risk Management,” press release, September 27, 2023, <https://news.chubb.com/2023-09-27-Chubb-and-SentinelOne-R-Partner-to-Enhance-Cyber-Risk-Management>.

108 At-Bay, “At-Bay Stance,” last accessed April 2025, <https://www.at-bay.com/stance/>.

109 Hiscox, “Cyber and Data Risk Solutions,” last accessed April 2025, <https://www.hiscox.com/documents/brokers/cyber/530-cyber-factsheet-broker.pdf>.

110 Chubb, “Explore U.S. Cyber Services,” last accessed April 2025, <https://www.chubb.com/us-en/business-insurance/products/cyber-insurance/us-cyber-services.html>.

111 Starr, “Securing your enterprise in the face of high-tech risks,” last accessed April 2025, <https://starrcompanies.com/Insurance/Casualty/Cyber>.

Examples

Not a comprehensive list, meant to illustrate what each of these incentives looks like in practice

Co-marketing partnerships

Cowbell Connectors: This program enables Cowbell to “connect to your infrastructure in a secure and restricted way and read limited information related to security controls and the use of security best practices.” Connectors produce insights that enable an insured to “improve its security posture resulting in better risk ratings and optimized premium and cyber insurance policy configuration.”¹¹²

Google Cloud Risk Protection Program: Cyber Insurance Hub, a security diagnostic tool, “scans your workloads on Google Cloud and provides proactive security recommendations to minimize misconfigurations, drive down risk, and boost security readiness.” The Hub then “generates a report that helps you understand your security risk posture on an ongoing basis and serves as an indicator of your security baseline, so you can identify where to route your security investments.” Partners with Beazley, Chubb, and MunichRe, which offer cyber insurance policies “designed exclusively for Google Cloud customers.”¹¹³

Bundled security services

Cowbell: For a fee, insureds can access Cowbell MDR SOC-as-a-Service, “powered by SpearTip, a company of Zurich Resilience Solutions, delivers a 24/7/365, U.S.-based Security Operations Center (SOC), staffed with certified, experienced engineers and analysts, providing real-time threat detection and AI-driven counterintelligence.”¹¹⁴

AXA XL: A partnership with Darkweb IQ’s Ransomware Detection & Response solution and Supply Chain Security+ offers “easy access and preferential pricing to its cyber security services.”¹¹⁵

Coalition: U.S. businesses that use 1) Coalition Managed Detection and Response, 2) CrowdStrike Falcon Complete, or 3) SentinelOne Vigilance Respond or Vigilance Respond Pro MDR solutions, which were “evaluated and hand-selected by experts on Coalition’s security and actuarial teams because they provide superior mitigation of cyber threats,” are eligible for a premium credit of up to 12.5%.¹¹⁶

Embedded policy features

Traveler’s Insurance: Insureds can access a complimentary one-hour consultation with the HCL Technologies Cyber Security Coach helpline at no additional cost, which “provides actionable advice and answers questions such as ‘What types of data should be encrypted?’ and ‘What are some best practices for security mobile devices?’”¹¹⁷

¹¹² Cowbell, “Cowbell Connectors,” last accessed April 2025, <https://cowbell.insure/cowbell-connectors/>.

¹¹³ Google Cloud, “Risk Protection Program: Key Features,” last accessed April 2025, <https://cloud.google.com/security/products/risk-protection-program>.

¹¹⁴ Cowbell, “Cowbell Launches Cowbell Resiliency Services (CRS) to Support U.S. Businesses As AI-Driven Cyber Threats Accelerate,” press release, February 4, 2025, <https://www.prnewswire.com/news-releases/cowbell-launches-cowbell-resiliency-services-crs-to-support-us-businesses-as-ai-driven-cyber-threats-accelerate-302367711.html>.

¹¹⁵ AXA XL, “AXA XL announces new partnership with Darkweb IQ to help businesses improve cyber security practices,” press release, March 6, 2025, <https://www.prnewswire.com/news-releases/axa-xl-announces-new-partnership-with-darkweb-iq-to-help-businesses-improve-cyber-security-practices-302393798.html>.

¹¹⁶ John B. Roberts, “Coalition is Now Offering Premium Credits to MDR Customers,” February 26, 2024, <https://www.coalitioninc.com/blog/premium-credits-mdr>.

¹¹⁷ Travelers, “Cyber Security Expert Coaching and Support Services,” last accessed April 2025, <https://www.travelers.com/business-insurance/cyber-insurance/cyber-support-services>.

Assessing Barriers and Concerns around Bundling

In theory, bundling stands to benefit all stakeholders involved. As more security companies recognize insurance as a vector through which to gain new customers, they could compete on the factor insurance values most: risk mitigation and management. For insureds, bundling could make it more affordable to access a product or service that ultimately helps them to improve their cybersecurity posture. For insurers, bundling could help them make inroads in new markets, opening up new opportunities for collaboration between cybersecurity products and services and cyber insurance, and could even reduce their overall risk exposure. Finally, insurance could help rearrange the incentive structure to push businesses towards better security practices, truly bolstering ecosystem-wide cyber resilience.

However, today's cyber insurance marketplace is far from this ideal, and does not feature many examples of bundling. If bundling could benefit all parties, why don't we see more of it?

Bundling has raised concerns in the past, particularly in the life insurance market of the late 19th century, when regulators worried that large rebates or discounts would distort the market and harm consumers. Anti-bundling rules were put into effect to address issues of insolvency, inaccurate risk assessment, and discrimination, which we address later on in this section. In today's environment, bundling can also create conflicts of interest between businesses that offer value-added services and insurance providers. It is first useful to examine current cyber insurance practices in this space before addressing the strengths and potential downsides of bundling.

Many cyber insurance providers offer minimal pre-breach, embedded policy services at no cost, such as an hour-long cybersecurity consultation or free access to services to help develop an incident response plan.¹¹⁸ Despite the information collected during the underwriting process about an insured's security status and levels of exposure to risk, often aided by security scans and self-questionnaires, many firms do not take an active role in helping insureds manage or mitigate that risk prior to a breach. Finally, many do not offer the option to bundle cyber insurance with additional security products or services that result in a reduced rate on the security product or service or a rebate on the policy premium. We suggest that underlying market dynamics, traditional insurance practices, and a shifting and opaque regulatory landscape have contributed to the dearth of bundling practices.

¹¹⁸ IST assessed the offerings from the top 20 cyber insurers, as well as other smaller cyber insurers, to understand the current pre-breach mitigation measures offered by each.

First, underlying market dynamics and traditional insurance practices may make the shift to a bundling model unappealing. Cyber insurance remains an under-explored line of insurance.¹¹⁹ Large insurance underwriters may offer cyber insurance to Fortune 500 companies, but they often do not write policies for SMEs. Insurers who already have a significant market share in other insurance verticals may see continued—but relatively small—potential for profit in cyber insurance, and therefore may be less likely to adopt innovative ways to manage or mitigate risk. Cyber risk behaves unlike most other perils: pricing a business’s level of cyber risk is difficult, but so is managing it. As a result, adapting an insurance model to offer pre-breach services that help to manage an insured’s level of cyber risk, either through in-house expertise or external vendor services, may not make sense for large traditional carriers, who already have market share and can write cyber insurance as part of a broader P&C offering. These underlying market dynamics could explain the number of “insurtech” entrants into the market—newer companies who take advantage of technology solutions, many of whom specialize in cyber insurance.¹²⁰

Whether cyber insurance is in the midst of a hard or soft market plays an important role as well. In hard markets, firms may be less likely to provide incentives to their insureds because they do not need to do so in order to gain customers. Indeed, offering cyber insurance alongside bundled security products or services could potentially cut down on a firm’s short-term revenue. In the long-term, however, this temporary loss of revenue could be offset by increased risk reduction and reduced claims, thus improving insurer profitability.¹²¹ Firms will need to be wary of competition, as another insurer could try to win over policyholders who have purchased bundled services and reduced their overall risk. This new firm could thus capitalize on the insured’s reduced risk profile and reduce the long-term profitability of the first firm, which initially invested in the bundled offering.

Reinsurance, or insurance for insurers, could also be acting as a constraint: given reinsurers’ exposure to the full extent of the risk pool, they may have less appetite for bundling. Reinsurers have been wary of the cyber insurance market given the volatility of loss ratios over the past decade. While reinsurance is playing an increasingly large role in the cyber market, reinsurers have tended to put in place fairly strict capacity limits for primary insurers.¹²² Even as the reinsurance market continues to expand, stringent capacity guidelines often

119 Manuel Adam and Koshiro Emura, “Cyber Insurance Market Outlook 2025: Cycle Management Will Be Key to Sustaining Profits,” *S&P Global*, November 27, 2024, <https://www.spglobal.com/ratings/en/research/articles/241127-cyber-insurance-market-outlook-2025-cycle-management-will-be-key-to-sustaining-profits-13323968>.

120 “Insurtech,” NAIC, last updated July 3, 2024, <https://content.naic.org/insurance-topics/insurtech>.

121 Angela Nieves, “Cyber Insurance Today: Saving It Before It Needs Saving,” *Catholic University Journal of Law and Technology* 29, no. 1 (2020), <https://scholarship.law.edu/jlt/vol29/iss1/4>.

122 Frank Cremer et al., “Enhancing cyber insurance strategies: exploring reinsurance and alternative risk transfer approaches,” *Journal of Cybersecurity*, Vol. 10, No. 1, 2024, <https://academic.oup.com/cybersecurity/article/10/1/tyae027/7920185>.

remain in place.¹²³ Indeed, many reinsurers view cyber insurance as both a major business opportunity and a major source of uncertainty. Reinsurers can benefit from increased data on the primary insurance market; if bundling provides mechanisms for insurers to gather more granular data from their policyholders, then that could prove to be a useful tool for expanding the reinsurance market. However, absent other mechanisms such as backstops or prudential regulations to address broader systemic risks in the cybersecurity ecosystem, bundling seems unlikely to significantly shift the reinsurance market.

An additional reason for the limited uptake in bundling may be state regulatory hurdles, whether real or perceived. Anti-rebating laws have been in existence since the late 19th century, prompted by concerns over life insurance agents who were offering rebates on policies to encourage customers to purchase life insurance from them—and in turn demanding higher commissions from the insurers. Some life insurers also combined insurance policies with added products or services unrelated to the insurance itself to induce customers to select one insurer or broker over another. This created concerns about market distortion, where the insurance products being purchased might not necessarily reflect the quality of the coverage or the financial health of the insurance firm, since individuals were signing up for policies based on the additional perks offered rather than the insurance policy itself. This practice also created concerns about market consolidation: smaller firms without the resources to provide products or services that might induce an individual to select that firm lost out to competitors with bigger budgets, regardless of product quality.¹²⁴

Massachusetts passed the first anti-rebating statute in 1887. Other states soon followed suit; by the early 1900s, most states had adopted some form of an anti-rebating law.¹²⁵ To align state approaches after the passage of the 1945 McCarran-Ferguson Act—a law that gave primary authority for regulating insurance to the states—the National Association of Insurance Commissioners put forward a model law targeting unfair competition and deceptive practices, which all states ultimately enacted.¹²⁶ Part of the model law focused on rebating and bundling.¹²⁷ In the context of the newly expanding personal life insurance market of the

123 Kenneth Araullo, “Cyber reinsurance market expands amid new capacity and competition – Lockton Re,” *Insurance Business Magazine*, January 30, 2025, <https://www.insurancebusinessmag.com/reinsurance/news/breaking-news/cyber-reinsurance-market-expands-amid-new-capacity-and-competition--lockton-re-522678.aspx>; Kristian McCann, “WTW: Cyber Risks Pushing Insurers to Scale Cover,” *Cyber Magazine*, December 20, 2024, <https://cybermagazine.com/articles/insurers-scale-facultative-cover-as-cyber-climate-risks-grow>.

124 Michael Griffin and Alan Levin, “You Can’t Get—Or Give—Something for Nothing: State Regulators Target Value Added Services Provided by Benefit Brokers,” *Federation of Regulatory Counsel Journal* 20, no. 2 (Summer 2009), <https://structuredsettlements.typepad.com/files/you-can-t-get---or-give---something-for-nothing.pdf>.

125 Jamie Parson, David Marlett, and Stuart Powell, “Time to Dust Off the Anti-Rebate Laws,” *Journal of Insurance Regulation* 36, no. 7 (2017), <https://content.naic.org/sites/default/files/jir-za-36-07-el-dust-off-anti-rebate.pdf>.

126 Baird Webel and Carolyn Cobb, “Insurance Regulation: History, Background, and Recent Congressional Oversight,” *Congressional Research Service*, February 2005, <https://www.everycrsreport.com/reports/RL31982.html>.

127 National Association of Insurance Commissioners, “Casualty and Surety Model Law,” proceeding 127, 1946; Michael Salinger, “Tying and Bundling in a Nearly Contestable Market,” May 2011, <https://www.ftc.gov/system/files/attachments/>

late 1800s, prohibiting rebating and bundling addressed three main concerns: insolvency, risk visibility and pricing, and anti-competitive behavior. In today’s landscape, bundling also raises a fourth concern around business-to-business relationships. In the following sections, we unpack each concern, discuss their current application in bundling broadly, and examine bundling of cyber insurance with security products and services specifically.

1. Insolvency

Regulators worried that an insurer, agent, or broker would offer so many rebates on their premiums that it would create a “race to the bottom” with their competitors, threatening the solvency of the industry.¹²⁸ Particularly since the 2008 financial crisis, developments in prudential regulation—risk-based legal measures that help ensure the financial stability and safety of institutions¹²⁹—have helped to mitigate many of these insolvency risks.¹³⁰ These risk-based measures include rate-filings, licensing procedures, corporate governance, and liquidity requirements and are intended to guard against the risk of insolvency. Specific to the insurance sector, insurers and regulators use catastrophe modeling software to track underlying exposure to correlated risk, regardless of whether the policies were distributed as standalone products or sold as a bundle. Prudential regulation is likely better placed to manage and control insolvency compared to restrictions on bundling, as measures like rate-filings, licensing procedures, corporate governance, and liquidity requirements thus far seem to more accurately and holistically measure risk concentration than restricting bundling.

In theory, bundling cybersecurity services with cyber insurance may even help to reduce risk exposure, since security offerings are intended to reduce the likelihood of cyber incidents occurring. In this way, bundled security services may help mitigate broader market solvency concerns by creating an additional avenue for avoiding massive cyber incidents: for example, a bundled cybersecurity company may be well-placed to notify insurance policyholders about zero-day vulnerabilities, thereby reducing the catastrophic risk associated with a threat actor exploiting those vulnerabilities at scale.

There are, however, caveats. Combining insurance with select security providers could push insureds toward the same few providers—such as a select or small group of Managed Detection and Response (MDR) firms—leading to risk concentration. If one of those providers

[bureau-economics-seminar-series-calendar-archive/111027salingerseminar.pdf](https://www.bureau-economics-seminar-series-calendar-archive/111027salingerseminar.pdf).

128 Ian Adams, “Anti-Rebating Laws and the Utah Experience,” R Street Institute, 2015, <https://www.rstreet.org/wp-content/uploads/2018/04/RSTREETSHORT8-1.pdf>.

129 Securities Industry and Financial Markets Association, “Prudential Regulation,” last accessed February 2025, <https://www.sifma.org/explore-issues/prudential-regulation/>.

130 Federal Reserve System, “Prudential Standards for Large Bank Holding Companies, Savings and Loan Holding Companies, and Foreign Banking Organizations,” 12 CFR Parts 217, 225, 238, 242, and 252, November 1, 2019, <https://www.federalregister.gov/documents/2019/11/01/2019-23662/prudential-standards-for-large-bank-holding-companies-savings-and-loan-holding-companies-and-foreign>.

is compromised, then an insurance firm who has bundled its insurance products with that provider could then face the prospect of paying too many claims at once, thus threatening its ability to stay solvent.¹³¹ Or if an MDR firm does not push out a patch of a zero- or n-day vulnerability quickly enough, then all of the firms using its services face exposure.¹³² The MDR space, while more diverse than other IT industries, still faces concentration risks.

Theoretically, bundling could also act as a countervailing force to risk concentration: security services like MDR would ideally help strengthen policyholders' security postures, ultimately reducing their exposure to attacks. Here, the question becomes one of weighing risks and benefits: the potential risk of a supply chain compromise against the potential benefits of increased resilience.

The problem of risk accumulation in the cybersecurity market is neither newly raised by nor unique to cyber insurance: the IT sector as a whole often faces questions of concentration risk, or "IT monoculture," in its supply chain.¹³³ The technology sector is often characterized by a few dominant firms, which is certainly true of operating systems and cloud computing. With the adequate caution and care, insurers could help play a role in reducing supply chain risk by guiding customers away from these dominant providers, given their attention to insolvency risk and prudential regulation. In the case of post-breach incident response, for example, some studies have shown that insurers increase diversity by negotiating rates with new, or more cost-effective, incident responders in the space.¹³⁴

2. Risk Assessment and Pricing

Regulators imposing initial anti-rebating laws also worried that rebating would impair insurers' understanding of the market, leading them to over- or under-price risk. In other words, in order to maintain a competitive market, insurers need to be able to see how their competitors assess and price risk. In the early days of life insurance, brokers sometimes sold policies with inducements that had nothing to do with the insurance offering itself, leading to market distortions. Insurers worried that their competitors' rebates would not be visible at the outset—preventing them from being able to price risk accurately and competitively.¹³⁵

131 To understand how risk concentration could lead to bad outcomes, Change Healthcare serves as a useful example. Vertical integration led to cascading failures. "Wyden Hearing Statement on Change Healthcare Cyberattack and UnitedHealth Group's Response," United States Senate Committee on Finance, press release, May 1, 2024, https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf.

132 John Banghart, "Risks Associated with IT Monoculture Needs Further Examination," Center for Cybersecurity Policy and Law, June 3, 2024, <https://www.centerforsecuritypolicy.org/insights-and-research/risks-associated-with-it-monoculture-needs-further-examination>.

133 John Banghart, "Risks Associated with IT Monoculture Needs Further Examination."

134 Woods and Böhme, "How Cyber Insurance Shapes Incident Response: A Mixed Methods Study."

135 Parson, Marlett, and Powell, "Time to Dust Off the Anti-Rebate Laws."

In the case of bundling, the combination of cybersecurity services with insurance could actually help insurers to gain a more complete understanding of the general market's levels of risk, as well as that of their competitors, so long as the value-added services are directly related to the insurance policy itself.

In addition to attempting to improve their understanding of the market level of risk, individual insurers have taken steps to improve their ability to price cyber risk.¹³⁶ As explored in [The Ransomware Era: New Forms of Security Assessment Emerge](#), the introduction of security assessments has likely improved underwriting. Insurers using security scans to conduct underwriting have been able to price premiums more quickly and sustainably, rather than conducting in-depth, time-consuming assessments of a prospective insured on a case-by-case basis.

Despite these improvements, traditional security scans have limitations: scans primarily assess external attack surfaces, may overlook the security posture of third- and fourth-party vendors, and ultimately fail to provide a full picture of an organization's security posture.¹³⁷ The next evolution of cyber underwriting could entail deeper visibility into internal cybersecurity controls. Bundling insurance with security services such as MDR could provide insurers with valuable real-time insights, improving both underwriting accuracy and risk mitigation. Ultimately, these insights could become valuable feedback for the insureds as they evaluate their policy decision-making processes and general security framework. As a result of this deeper visibility into the security posture and risk level of a prospective insured, insurers could then more accurately price risk, avoiding the over- or under-pricing of risk that early regulators sought to prevent.

In considering whether bundling impairs visibility of the market, insureds must weigh the tradeoffs of different bundling structures, including the differences between an in-house value-added product or service offered by an insurer or its affiliate and an external value-added product or service offered by a third-party provider. An insurer may be able to hone its own products with real-time data, but the practice could lead to less overall market transparency, as competitors will not be able to gauge the findings or quality of an in-house service in the same way they may be able to evaluate a third-party service. Yet IT services are already concentrated in a small number of firms, and insurers can be a mechanism for breaking up consolidated markets. As explored in the next section, a healthy market will likely need to reflect a diverse range of bundling structures to avoid issues of market capture.

¹³⁶ Zoë Brammer, "Putting the Blueprint for Ransomware Defense to the Test," Institute for Security and Technology, August 28, 2023, <https://securityandtechnology.org/blog/putting-the-blueprint-for-ransomware-defense-to-the-test/>; Coalition, "Coalition Cyber Threat Index 2025," March 2025, <https://www.coalitioninc.com/blog/cyber-threat-index-2025>.

¹³⁷ Talesh and Cunningham, "The Technologization of Insurance."

3. Discriminatory Practices

Early regulators also sought to eliminate the possibility of discrimination, or that an insurer, agent, or broker would offer a rebate to one customer over another on an unrelated, arbitrary basis.¹³⁸ In the case of discrimination against insureds or prospective insureds, value-added services should be offered to all, regardless of security status or other arbitrary bases. Here, model regulation proposed by NAIC can be a useful starting point for preventing discrimination against insureds.¹³⁹

Bundling raises additional concerns related to discrimination in the marketplace of the non-insurance service or product: an insurer could decide to partner with one firm over another on an arbitrary or unrelated basis. When it comes to discrimination concerns in the marketplace that might lead an insurer to bundle non-insurance, value-added products or services in a discriminatory manner, it is important to consider the state of the cybersecurity services marketplace. Unlike the market for vehicles or other consumer products, the cybersecurity marketplace is underdeveloped, with a lack of product certifications and commonly agreed-upon standards. The IT sector has not undergone the shift toward products that are “safe by design” that has occurred for other physical products.¹⁴⁰ In the security services marketplace, there is no comparable scheme.¹⁴¹ Secure by design initiatives are also working to shift the market toward better security practices, but remain nascent.

Given this lack of common standards or certifications, cyber insurers would be acting irresponsibly if they relied solely on prevailing market forces (which can be a result of IT monoculture) or other unrelated or arbitrary measures to select the security providers with whom to bundle products and services. To the extent that insurers can identify top-tier security providers, the practice of guiding insureds towards the most cost-effective provider could prove to be a positive development for businesses and the broader sustainability of the

138 Griffin and Levin, “You Can’t Get—Or Give—Something for Nothing.”

139 National Association of Insurance Commissioners, “Model Law 880,” Section 4(H): 4-5.

140 Manufacturers of products like vehicles, food, or airplanes must prioritize safety by design to ensure that they function properly when used as intended, including through the invention and production stages. United States Consumer Product Safety Commission, “Manufacturing Best Practices,” last accessed February 2025, <https://www.cpsc.gov/business--manufacturing/business-education/business-guidance/BestPractices>.

141 In contrast to the dominance of the safety by design paradigm in the physical manufacturing space, security by design is not universally adopted throughout the cybersecurity ecosystem. The idea of secure-by-design IT is not new. See: Jerome Saltzer and Michael Schroeder, “The Protection of Information in Computer Systems,” in *Proceedings of the IEEE* 63, no. 9 (September 1975), <http://www.cs.virginia.edu/~evans/cs551/saltzer/>. However, it has recently gained more traction in policy circles. See: Cybersecurity and Infrastructure Security Agency, “Secure-by-Design,” October 25, 2023, <https://www.cisa.gov/resources-tools/resources/secure-by-design>; Sezaneh Seymour and Daniel Woods, “Calibrating Secure by Design with the Risks Faced by Small Businesses,” *Lawfare*, February 14, 2025, <https://www.lawfaremedia.org/article/calibrating-secure-by-design-with-the-risks-faced-by-small-businesses>; Scott Shackleford et al., “The Difficulties of Defining ‘Secure-by-Design,’” *Lawfare*, February 6, 2024, <https://www.lawfaremedia.org/article/the-difficulties-of-defining-secure-by-design>.

market. In addition to market forces, insurance bundling practices should be balanced with appropriate regulatory oversight in order to avoid anti-competitive results.

Beyond guiding customers towards existing providers, insurers have also turned to in-house security services (e.g., provided by affiliates or subsidiaries) as a form of bundling. This form of partnership should raise the most regulatory scrutiny, given the potential conflict of interest. However, if regulated carefully, this model could produce potential benefits by creating easy information-sharing mechanisms and addressing gaps in the market. Regulation to address this potential conflict of interest should consider the general financial health of the firm and its fiduciary duties to clients, as well as appropriate disclosure obligations.

In terms of information exchange, insurers operating in-house security services could feed lessons learned from managed detection and response into improving underwriting. For example, observing that threat actors repeatedly use a specific technology to move laterally through a network could result in asking new underwriting questions around how prospective insureds configure that technology. Going the other way round, insurers could more easily feed lessons from insurance claims into an in-house provider's services. Finally, in-house providers could be better able to integrate with the insurer, for example by directly acting on vulnerability notifications or threat intelligence.

Insurers could also create in-house solutions that are not available on the market. For example, many MDR solutions are targeted at large customers with thousands of machines to monitor. Small businesses may not have enough machines to qualify for the minimum contract size, which could motivate insurers to create in-house options to fill this gap. Similarly, insurers could be able to create lower cost solutions, given they can save on marketing costs. Here, again, regulation is key to mitigating conflicts of interest.

4. Conflicts of Interest in Business-to-Business (B2B) Relationships

Bundling provides new opportunities for insurers to develop close relationships with external, value-added service providers (or with their own in-house service provider), which raises an additional concern: business-to-business (B2B) relationships. This paper has thus far stressed the many opportunities that these relationships offer to help insureds strengthen their security postures, particularly in a field like cybersecurity that does not have strong external benchmarking and standards. Sending insureds to *some* service or product to improve their cybersecurity may be better than the status quo.

However, insurance companies stand to gain market share by partnering with external vendors, who can help to direct clients back to their insurance products. These bundled

offerings present a valuable sales opportunity for insurers—a factor that makes bundling compelling, but that also raises possible conflicts of interest. While insurers want to reduce the amount they pay in claims, they also want to offset other overhead costs, including their sales and marketing departments. Insurers may not always be incentivized to pursue the value-added services with the strongest cybersecurity, but rather the bundled products that create the most opportunity for increased market penetration and profit maximization.

To address this concern, regulators should carefully consider rules that offer consumer protection against unfair business practices, including appropriate disclosure requirements and customer data protections. For example, an insurer might be required to report to state regulators the terms of the business-to-business agreement and any kick-backs they may be receiving. Or, an insurer might be required to disclose to brokers and prospective insureds the terms of the business-to-business relationship prior to the purchase of a bundled product or service. Overall, bundling presents an important new avenue for incentivizing cybersecurity among insureds, but regulators must be wary of the kind of B2B relationships that may distort outcomes for consumers. In the long term, insurers and insureds can both benefit from upfront cybersecurity investments that bolster a policyholder's security posture and reduce the likelihood of incidents and the impact should one occur.

Bundling also raises concerns around vertical integration of the cyber insurance industry, whereby one major player begins to dominate insurance and security for insureds across the entire supply chain. This kind of market capture can lead to unfair or discriminatory pricing practices, de facto insurer lock-in (as insureds have deployed a particular security service already and may be reticent to shift to another service that can be bundled with other insurers), or other adverse market capture.

Bundling Today: Current barriers to adoption

In recent years, both the National Association of Insurance Commissioners (NAIC) and the National Conference of Insurance Legislators (NCOIL) have initiated conversations on anti-rebating, of which bundling is one primary example.¹⁴² Starting in 2018, NAIC's Innovation Cybersecurity and Technology Committee took up a review of the model law's anti-rebating statutes "particularly because of the increased interest in offering value-added products and services such as risk mitigation devices and related services that are not necessarily addressed within the applicable insurance policy language."¹⁴³ Following presentations and

¹⁴² The National Council of Insurance Legislators (NCOIL) works alongside NAIC and is primarily responsible for collaboration with state-level legislators.

¹⁴³ National Association of Insurance Commissioners, "Project History 2024: Amendments to the Unfair Trade Practices Act," 2024, <https://content.naic.org/sites/default/files/model-laws-project-history-880.pdf>.

testimony from stakeholders across the insurance ecosystem, a committee of state legislators, industry representatives, the president of NCOIL, and a consumer representative led drafting of the amended model law. After an open comment period on the revised draft and a series of revisions, the NAIC Executive Committee voted unanimously to adopt the new model language in December 2020.¹⁴⁴

The new model law allows for the provision of value-added services or products “at no or reduced cost” even when not specified in the policy as long as they relate to the insurance coverage and are primarily designed to: provide loss mitigation or loss control, reduce claim costs or claim settlement costs, provide education about risk of loss, monitor/assess risk, identify sources of risk, develop strategies for eliminating risk, or provide post-loss services. To reduce the risk of discriminatory practices, the model law specifies that insurers must make these bundled services available to insureds as a value-added product based on documented, objective criteria. The model law states that the cost of the bundled product or service must also be reasonable compared to the premium cost. To address concerns over consumer protection, the model law also instructs commissioners to adopt regulations, “consistent with applicable law, [which] may address, among other issues, consumer data protections and privacy, consumer disclosure and unfair discrimination.”¹⁴⁵

The current status of state-level anti-bundling laws is quite varied. Importantly, the NAIC and NCOIL model laws are just that—models. Each state ultimately makes the decision of whether or not to lift existing prohibitions on bundling and change the language. Furthermore, a state may not adopt the full text of the model law or may carve out exceptions through legal precedent. As of January 2025, we assess that 25 states have lifted some form of prohibitions on bundling, while some version of the prohibition on bundling insurance with value-added services remains in place in 25 states and the District of Columbia.¹⁴⁶

Even though some states do allow for bundling, the current patchwork of legislation—coupled with the broadly (mis)understood legal precedent related to anti-rebating and anti-bundling—makes it more challenging for an insurer to leverage bundling as an opportunity. This may have a chilling effect on firms’ willingness to move into this space. Rather than track bundling laws in every jurisdiction to make sure they remain in compliance, insurers may choose to forgo bundling altogether, sticking to the lowest common denominator: no bundled services or

144 National Association of Insurance Commissioners, “Project History 2024: Amendments to the Unfair Trade Practices Act.”

145 National Association of Insurance Commissioners, “Unfair Trade Practices Act,” Model Law 880-1.

146 As of January 25, the 25 states (plus the District of Columbia) that still have some version of a prohibition on bundling are Alaska, Colorado, DC, Delaware, Georgia, Hawaii, Idaho, Louisiana, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, Oklahoma, Oregon, South Carolina, Tennessee, Texas, Vermont, Virginia, Washington, and Wisconsin. The 25 states that have, to some extent, lifted prohibitions on bundling and updated their laws or issued guidance to account for value-added services are Alabama, Arizona, Arkansas, California, Connecticut, Florida, Illinois, Indiana, Kansas, Kentucky, Maine, Minnesota, New Hampshire, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island, South Dakota, Utah, West Virginia, Wyoming, New Mexico, North Dakota, and Iowa.

products at all. As two lawyers on a podcast episode discussing these practices say, “We don’t generally advise rebating.”¹⁴⁷

Even if an insurer would like to offer bundling to their insureds, they may be advised against it by others involved in managing their risk pool, including reinsurers, who may take a different view of the regulations or a different stance on the level of legal ambiguity they are willing to accept. Finally, the definition of bundling can vary, depending on the law being referenced or the exact circumstance. As a result, some insurers may take a narrower approach to the definition, such as applying it only to the bundling of third-party, external security services with insurance, while others may be more inclined to take an all-inclusive approach, such as including the bundling of both third-party and internal security services with insurance. This variation in the practical interpretation of bundling also hinders broader adoption across the ecosystem.

Proponents of bundling argue that these prohibitions stifle innovation and competition among firms. According to the strictest interpretation of the law, these statutes prevent a firm from offering any combination of insurance with non-insurance products or services, which proponents argue ultimately hurts consumers and prevents firms from being able to incorporate technological solutions into their offerings.

In summary, navigating the concerns raised around bundling with its potential benefits requires careful oversight. Regulators can promote transparency in bundling arrangements by providing non-binding guidance to the market while also issuing clear rules to prevent unfair practices. Ultimately, regulators should aim to balance cybersecurity effectiveness with market choice—giving policyholders access to high-quality security solutions without unduly restricting competition, introducing discrimination, impairing the ability to price risk, threatening insolvency, or introducing anti-competitive business-to-business relationships. With proper attention and regulation to address these risks, bundling has the potential to enhance cyber resilience at the individual organization level and, more broadly, to generate significant public benefits.

¹⁴⁷ Robert Tomilson and Scott Galla, “Anti-Rebating Statutes,” Insurtech Briefly podcast, November 12, 2021, <https://www.jdsupra.com/legalnews/insurtech-briefly-podcast-anti-rebatin-09070/>.

Recommendations

Cyber insurance has the potential to play a larger role in proactive risk management and mitigation and to achieve the bold vision Schneier described over two decades ago.

While further research is necessary, bundling could help policyholders overcome certain cybersecurity market information asymmetries and create meaningful security benefits for insurers, policyholders, and the broader cybersecurity ecosystem. To enhance cyber resilience and encourage cybersecurity from the outset, cyber insurance could make pre-breach cyber risk mitigation a more prominent feature of the cyber insurance marketplace. Specifically, this piece recommends examining bundling as a possible path forward through the following three avenues.

Recommendation 1: Regulators and policymakers should encourage cyber insurers to present policyholders with more proactive pre-breach risk mitigation tools and strategies, including by bundling insurance with security products and services.

The combination of insurance with value-added products and services can help insurers to manage an insured's risk levels, reduce future claims, and even gather more information to support future risk mitigation tactics—ultimately helping businesses and organizations become more cyber resilient.

As this research highlights, regulatory uncertainty at the state level may discourage insurers from implementing bundling. Even in jurisdictions where existing laws are permissive, uncertainty about regulators' positions on pre-breach, proactive risk mitigation may have a chilling effect on insurer innovation.

By fostering a regulatory environment that supports proactive cyber risk mitigation and bundling specifically, states can enhance both business resilience and broader market stability.

We recommend that state departments of insurance seeking to encourage cyber insurers to adopt proactive cyber risk mitigation strategies send positive signals to the marketplace, including by adopting some or all of Model Law 880. State departments of insurance should encourage insurers to:

- » Clearly communicate to policyholders that enhancing their security posture can directly improve their risk profile and may qualify them for lower premiums.

- » Provide tailored education to policyholders on security measures and services that align with their specific risk profiles, helping them make informed decisions about risk mitigation.
- » Consider opportunities to bundle cyber insurance with complementary security products or services by partnering with insurer affiliates or third-party security providers, thereby offering policyholders more comprehensive protection.

One of the provisions of the NAIC Model Law stipulates that the “cost to the insurer or producer offering the product or service to any given customer must be reasonable in comparison to that customer’s premiums or insurance coverage for the policy class.”¹⁴⁸ This caveat regarding costs being reasonable in relation to the premium cost may have introduced some uncertainty or reluctance in the market, as the cost of value-added cybersecurity risk mitigation services such as MDR can exceed the costs of annual insurance premiums. In states that have adopted this language, they may wish to clarify or confirm that the law allows value-added measures to be reasonable in cost relative to comparable market offerings within a given policy class. This clarification is relevant to the cyber insurance market, where risk mitigation solutions can be costly yet provide significant value.

Recommendation 2: Researchers should conduct additional analysis to improve the understanding of bundling as a model, take a deep dive into a select few firms that offer bundled services and a few insured SMEs or SLTTs that have taken up those services, and explore why more firms do not.

As explored in Section V, some insurers have begun taking a more innovative approach to proactive security for their insureds, exploring new options that bundle third party or in-house risk management and mitigation with an insurance policy, and even sometimes offering reduced rates on security products and services or rebates on the insurance premium. Because the practical application, adoption, and outcomes of bundling continue to be a topic of debate, we recommend a case study focused on a small number of insurers currently offering some form of bundling, including reduced rates on in-house and external security services and rebates rewarding insureds through the use of their value-added products and services.

- » **Incentive structure:** The case study could investigate the specific types of incentives offered, including discounts, rebates, and value-added services. It could create a clearer picture of the current status of bundling in the insurance marketplace, articulating the full range of possibilities when it comes to bundling. The case study should also examine insurer incentives, including the structure of vendor-insurer relationships.

¹⁴⁸ NAIC Model Law, Section 4.H.1.2.(e)(iii).

- » **SME adoption:** As explored in this paper, a majority of large businesses hold cyber insurance, compared to only a small minority of SMEs. In addition, unlike large corporations, SMEs are more likely to be under-resourced for cybersecurity. In theory, bundling is one way to increase adoption of cyber insurance for SMEs and to incentivize them to boost their levels of cyber resilience. A case study of cyber insurance providers who bundle insurance with security products and services could investigate the uptake of bundling for small and large businesses, putting this theory to the test. This could also be an opportunity to investigate what SMEs would like to see from their insurers, which could include left-of-boom preventative services.
- » **Outcomes:** A case study could also offer more evidence on the outcomes of bundling, comparing the rate of breaches in insureds who do not use bundled proactive security services with those who do.
- » **Barriers to bundling implementation:** For those firms that do not currently offer bundled services or discounts, further research could also explore why they do not. This piece theorizes that market dynamics may make the shift to a bundling model unappealing for large insurance underwriters. Further research could explore this argument through targeted interviews or workshops.

Recommendation 3: Researchers should compare outcomes between states that allow bundling, and states that do not.

Current state approaches to bundling vary: many states have revised their laws to permit bundling in one form or another, while others have not. Further research could compare the regulatory landscape and bundling outcomes on a state-by-state basis to understand the actual effects, explore additional regulatory guardrails, and understand how to effectively implement bundling given the uniqueness of the cyber risk space.

For example, as articulated in Section VI, bundling raises concerns over the consolidation of the security services marketplace, the concentration of risk in one or a few service providers, the potential for discrimination, and conflicts of interest arising from insurer partnerships with security vendors (B2B relationships). Research comparing states that allow bundling to states that restrict bundling and rebating could evaluate to what extent these concerns are borne out in reality, evaluating the levels of consolidation in the marketplace, the levels of insolvency risk involved, and the effect on insureds. Research could also assess alternative regulations that could—or perhaps already do—guard against insolvency, discrimination, or inaccurate risk pricing and protect consumer interests.

Prior research has pointed to the cases of California and Florida, where amendments passed in 1988 and 1990 allowed rebating with specific exceptions.¹⁴⁹ In its decision, Florida’s Supreme Court wrote, “[t]he anti-rebate statutes... simply deprive the consuming public of a choice in the price of products or services, the choice of which is the cornerstone of a competitive, free-market economy.”¹⁵⁰ In the cases of both California and Florida, the fears expressed by opponents of anti-rebating reform—specifically that it would create insurer insolvency, impair insurer’s understanding of the market, or lead to discriminatory practices—have yet to be realized. Some argue that these outcomes have not arisen because other laws and regulations now guard against those concerns without targeting rebating specifically, including rate-filings, licensing procedures, risk-based capital standards, and other legal anti-discrimination measures.¹⁵¹ Regardless, cyber insurance itself is newer than both anti-rebating laws and their subsequent rollback in some states, making such conclusions hard to draw.

This line of effort could also help point regulators to additional stipulations that would prevent worst-case scenarios. For example, in order to prevent conflicts of interest between insurers and in-house security services firms, regulators might allow insurers to offer discounts for their own security service affiliates provided that they also identify and extend discounts for other top-tier providers to ensure a competitive market.

Finally, as this research identified, regulatory hurdles—real or perceived—have prevented insurers from adopting widespread bundling practices, including the provision of value-added services that do not need to be specified in the policy itself. We recommend that further research investigate how states are approaching bundling generally, exploring the broad concerns raised by state legislators and insurance commissioners in each state, and examining how each of these broad concerns applies to the cyber insurance space.

Conclusion

As a practice, bundling is not without its limitations or possible drawbacks. When it was first introduced in the late 1800s, it was used in a market—life insurance—that was already rife with confusion and controversy. Brokers and agents had to find a way to convince individuals to buy their policies, with very few guarantees about what might happen in the intervening years or decades between purchase and payout. Inducements, rebates, and bundles were a powerful sales technique, albeit one that could breed market distortion and anti-competitive practices.

149 Parson, Marlett, and Powell, “Time to Dust Off the Anti-Rebate Laws;” Adams, “Anti-Rebating Laws and the Utah Experience.”

150 Supreme Court of Florida, “Department of Insurance vs. Dade County Consumer Advocate’s Office,” 49 So. 2d 1032, 1986, <https://law.justia.com/cases/florida/supreme-court/1986/66178-0.html>.

151 See: Adams, “Anti-Rebating Laws and the Utah Experience.”

The insurance market today looks much different. Policymakers have introduced prudential regulations, disclosure policies, and other mechanisms for protecting consumers and safeguarding the health of insurance industries. Cyber insurance may be a newer, underexplored line of P&C insurance, but it is not starting from a blank slate; it is subject to the guardrails that have evolved over the last century.

Bundling security services with cyber insurance poses a unique opportunity to align long-term incentives between insurers and insureds, ultimately bolstering policyholder cybersecurity and cyber hygiene. Bundling can also foster unique insights into the way specific security controls affect security outcomes; insurers with access to claims data could be in a privileged position to evaluate what works (and what does not), and could even help push insureds to pursue more efficient, more effective practices.

As this paper explores, bundling does raise specific questions about insolvency, risk visibility and pricing, anti-competitive behavior, and conflicts of interest arising from relationships between insurers and security vendors. This paper outlines several ways that these concerns can be studied more closely, including through investigations of bundling practices and comparative studies of bundling by state, and mitigated, including through prudential regulation and disclosure obligations. Ultimately, we conclude that regulators and policymakers should encourage cyber insurers to present policyholders with more proactive pre-breach risk mitigation tools and strategies, including bundling.

This paper identifies additional aspects for further exploration and evaluation in the cyber insurance market. Due to challenges with systemic risk modeling, government may be well-positioned to intervene in the reinsurance market to attenuate tail risk. Mapping the insurance ecosystem could also be a useful starting point to understand how brokers, insurers, and reinsurers interact with each other and to pinpoint where bundling and other possible market-based solutions can be helpful mechanisms for incentivizing security practices. This paper marks a first foray into the world of bundling—one which we hope will spark more discussion about the role of cyber insurance in realizing cyber resilience, and the potential of bundling as one avenue towards cyber resilience for SMEs and SLTTs in particular.



INSTITUTE FOR SECURITY AND TECHNOLOGY

www.securityandtechnology.org

info@securityandtechnology.org

Copyright 2025, The Institute for Security and Technology