Revolutionizing Cyber Insurance

LOWERING COSTS AND ENHANCING RESILIENCE WITH BLUE TEAM ALPHA

BLUE TEAM ALPHA

Author:
Jonathan Krasner, Director of Strategic Alliances, Blue Team Alpha

Contents

SECTION 1: CHALLENGES AND REQUIREMENTS IN THE CYBER INSURANCE INDUSTRY

SECTION 2: THE ROLE OF CYBER CONTROLS AND IMPLICATIONS FOR CYBER INSURANCE

SECTION 3: CONCLUSION AND FUTURE OUTLOOK

SECTION 1: CHALLENGES AND REQUIREMENTS IN THE CYBER INSURANCE INDUSTRY

Introduction

The cyber insurance industry has experienced exponential growth in recent years, with a projected compound annual growth rate (CAGR) of 16.40% expected to propel it to reach US $20.432 billion by 2027[1]. This growth can be attributed to organizations' increasing efforts to safeguard themselves against the ever-escalating threat of cyberattacks. The NETDILIGENCE® CYBER CLAIMS STUDY 2022 REPORT indicates that carriers are facing the need to control claim expenses as loss ratios in the cyber insurance industry exceed 60-75% and continue to rise[2].

$20.43 BILLION

Projected value of the cyber insurance market by 2027.

The traditional incident response model and the increasing cost of cyber insurance claims have presented significant challenges for insurers and policyholders. In this whitepaper, we propose a new approach that addresses these challenges and revolutionizes the industry.

Challenges in the Cyber Insurance Industry

"CYBER LIABILITY CLAIMS SURGED BY 75% IN 2022 COMPARED TO THE PREVIOUS YEAR"

The cyber insurance industry faces significant challenges despite the increasing demand for coverage. One major obstacle is the rising cost of cyber insurance claims, which can be attributed to the ever-evolving nature of cyberthreats and the sophistication of cyberattacks. Incident response costs, including recovery costs, legal fees, forensic investigations, and public relations efforts, have escalated as a result. This has made it difficult for insurers to accurately assess and price cyber-risk, resulting in higher premiums, higher deductibles, coverage erosion and lower over-limits for policyholders. According to a report by Willis Towers Watson, cyber liability claims surged by 75% in 2022 compared to the previous year[4].

Insurers' Requirements and the Role of Cyber Controls

Insurers increasingly require organizations to invest in cyber controls as a condition for obtaining cyber insurance policies. This requirement stems from the understanding that implementing effective controls can mitigate risks and reduce the likelihood and severity of cyber incidents. By incentivizing organizations to implement cyber controls, insurers aim to minimize the number of claims and lower the average claim cost by promoting enhanced security measures[7].

While there is no universal set of requirements that applies to all cyber insurance policies and businesses, certain controls are commonly sought by insurers during the underwriting or policy renewal process.

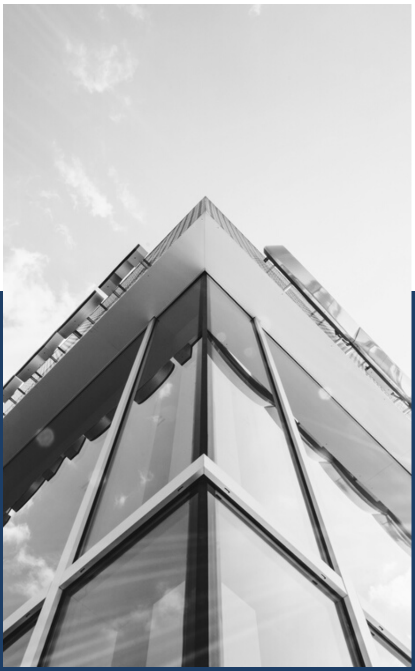
Insurers often look for the following cyber controls:

- Endpoint detection and response (EDR) implemented on all endpoints to minimize the risk of unauthorized access and malware infections[7].
- Multi-factor authentication (MFA) enabled for all remote access and cloud services to prevent credential compromise and account takeover[7].
- Regular backups of critical data and systems, preferably offline or in the cloud, to ensure business continuity and recovery in case of ransomware or data loss[7].
- Encryption of sensitive data at rest and in transit to protect it from unauthorized access or disclosure[7].
- Security awareness training for all employees to educate them on cyber threats and best practices[7].
- Vulnerability scanning and patch management to identify and fix security weaknesses in the network and systems[7].
- •Firewall and antivirus software installed and updated on all devices to block malicious traffic and detect known malware[7].
- Incident response plan and team to prepare for and respond to cyber incidents effectively[7].
- Compliance with relevant laws and regulations regarding data protection and privacy, such as GDPR or HIPAA[7].

These requirements help ensure that the organization has a baseline level of security to reduce the likelihood and impact of cyber incidents. However, they are not a guarantee of protection or coverage.

Factors Considered for Cyber Insurance Eligibility

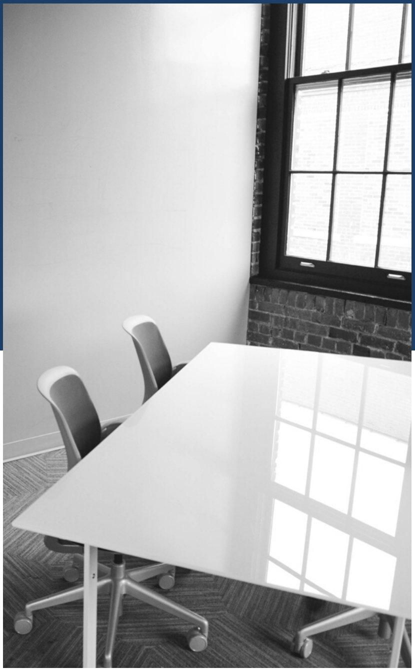
Cyber insurers consider several factors when determining the eligibility, scope and cost of a cyber insurance policy. Therefore, it is crucial for businesses to consult with their insurance agent or broker to understand what cyber insurance policy would best fit their needs and expectations.



These factors include:

- **Size:** The organization’s size is assessed to gauge its risk profile and coverage needs.
- **Industry:** Different industries have varying levels of cyber-risk, leading to tailored requirements from insurers.
- **Revenue:** Insurers consider the financial capacity of an organization to handle cyber incidents and claims.
- **Claims History:** Previous claims or incidents impact the perceived risk of the organization.

  Risk Appetite: Insurers evaluate the organization's attitude towards risk and commitment to robust controls.



There is a noticeable trend among cyber insurance companies to require cyber controls for policy eligibility. While different insurers may have different policies and criteria, the industry is becoming more selective and demanding regarding the security practices and controls expected of policyholders.

SECTION 2: THE ROLE OF CYBER CONTROLS AND IMPLICATIONS FOR CYBER INSURANCE

Emphasis on Cybersecurity Measures

Reports from reputable sources highlight the increasing scrutiny of cyber insurers regarding the security practices of policyholders. The National Association of Insurance Commissioners (NAIC) report emphasizes that insurers are placing a higher emphasis on cybersecurity measures due to the rise in ransomware attacks and associated losses[12]. Insurers now request more comprehensive information and evidence of cyber controls from their clients. These controls include endpoint detection and response (EDR), multi-factor authentication (MFA), secure backups, network access controls, content filtering, patch management, incident response planning, and cybersecurity awareness training[13].

Demanding Stricter Cybersecurity Hygiene

The Cyber Insurance Academy report further supports the notion that cyber insurers are demanding stricter cybersecurity hygiene from their clients. They have compiled a list of minimum requirements that most insurers expect, such as EDR, MFA, backups, encryption, security training, vulnerability scanning, firewall and antivirus software, incident response plans and teams, and compliance with relevant laws and regulations[14].

Considering these sources collectively, it can be inferred that a significant percentage of cyber insurers now require cyber controls to obtain a policy. The exact percentage may vary depending on market conditions and data sources. However, this trend is expected to continue or potentially increase as cyber-risks become more prevalent and complex.

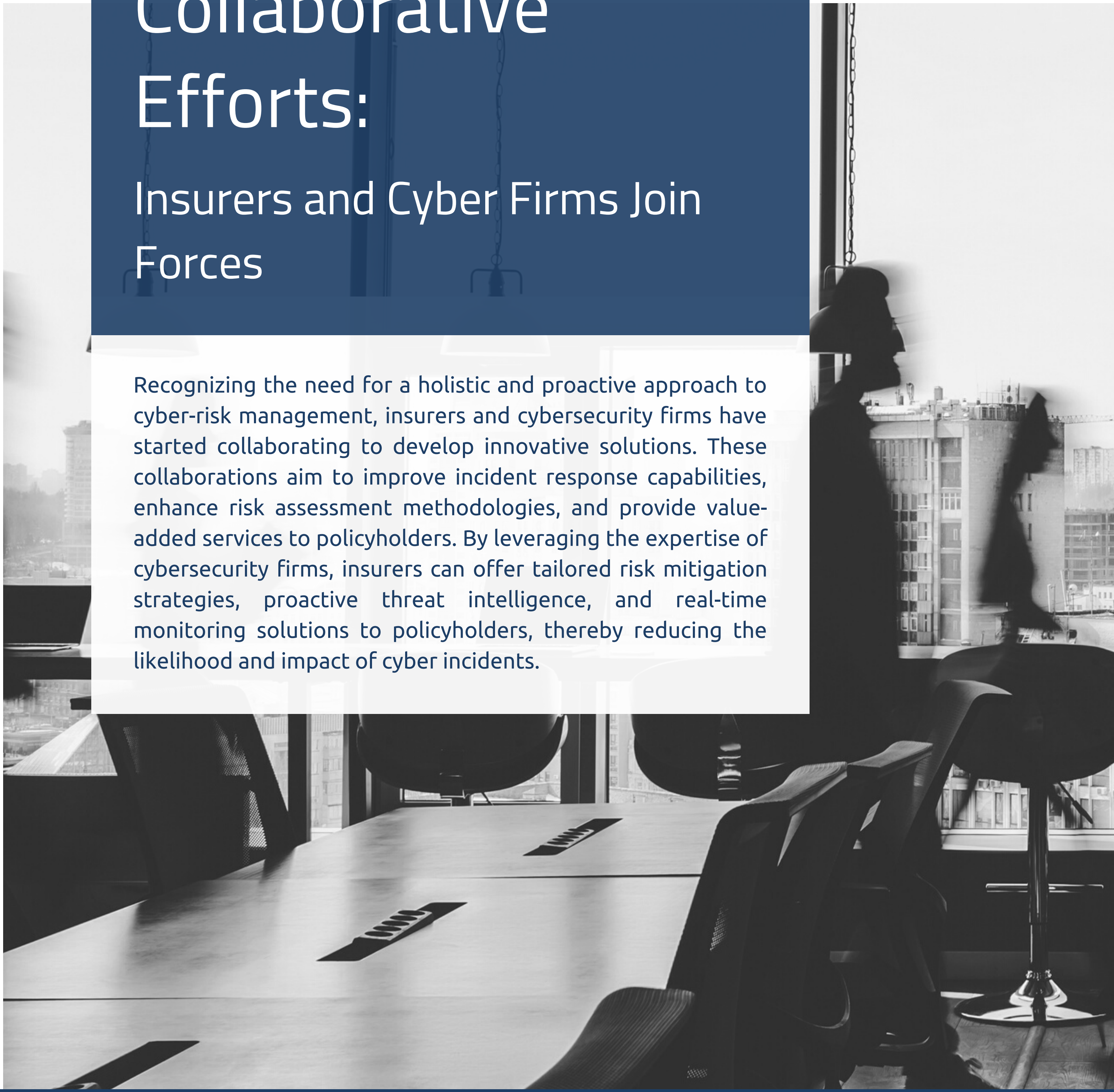
> **By implementing robust cyber controls and adhering to industry best practices, organizations can improve their chances of obtaining cyber insurance coverage and potentially secure more favorable policy terms.**

As a result, organizations seeking cyber insurance should be prepared to demonstrate their cybersecurity posture and maturity to potential insurers. By implementing robust cyber controls and adhering to industry best practices, organizations can improve their chances of obtaining cyber insurance coverage and potentially secure more favorable policy terms.

Collaborative Efforts:

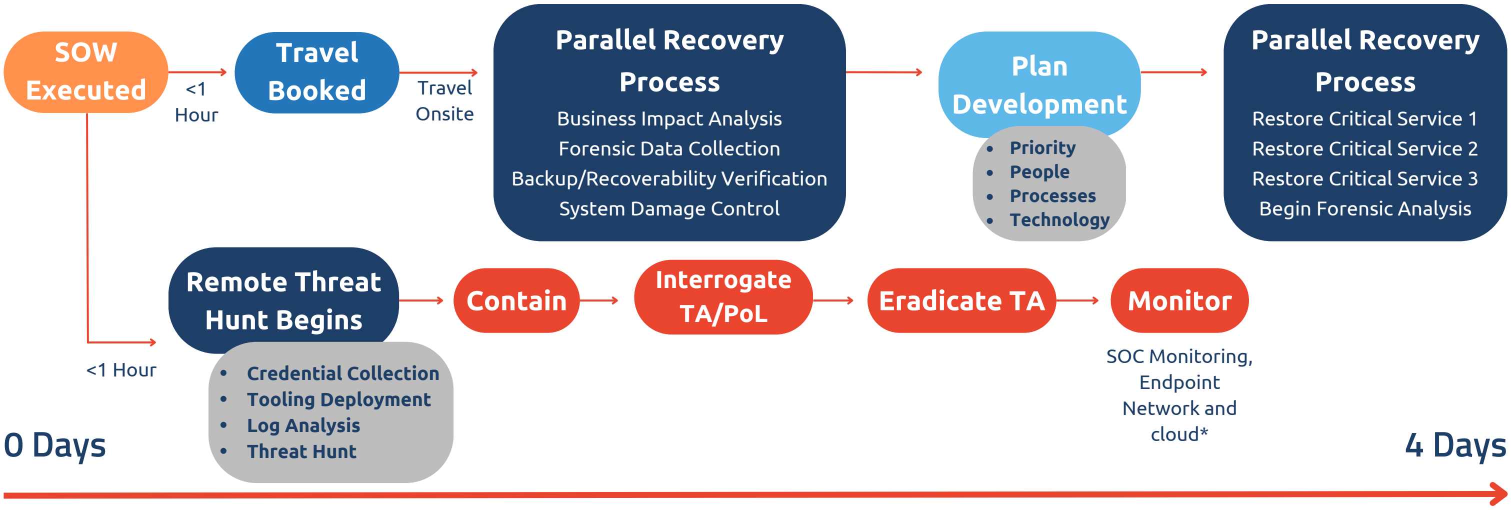
Insurers and Cyber Firms Join Forces

Recognizing the need for a holistic and proactive approach to cyber-risk management, insurers and cybersecurity firms have started collaborating to develop innovative solutions. These collaborations aim to improve incident response capabilities, enhance risk assessment methodologies, and provide value-added services to policyholders. By leveraging the expertise of cybersecurity firms, insurers can offer tailored risk mitigation strategies, proactive threat intelligence, and real-time monitoring solutions to policyholders, thereby reducing the likelihood and impact of cyber incidents.



The Parallel Incident Response Model by Blue Team Alpha

Traditionally, incident response processes have several issues that prolong the response time. One major drawback is the serial execution of steps, such as forensics investigation, response coordination, and recovery, which leads to increased downtime and higher costs for organizations and insurers. Conducting forensics before initiating the response is also a common practice that further contributes to the delay in recovery[7]. Additionally, the involvement of breach coaches, typically lawyers, can introduce additional time constraints and hinder the swift response process.



Average Timeline to Critical Service Restoration

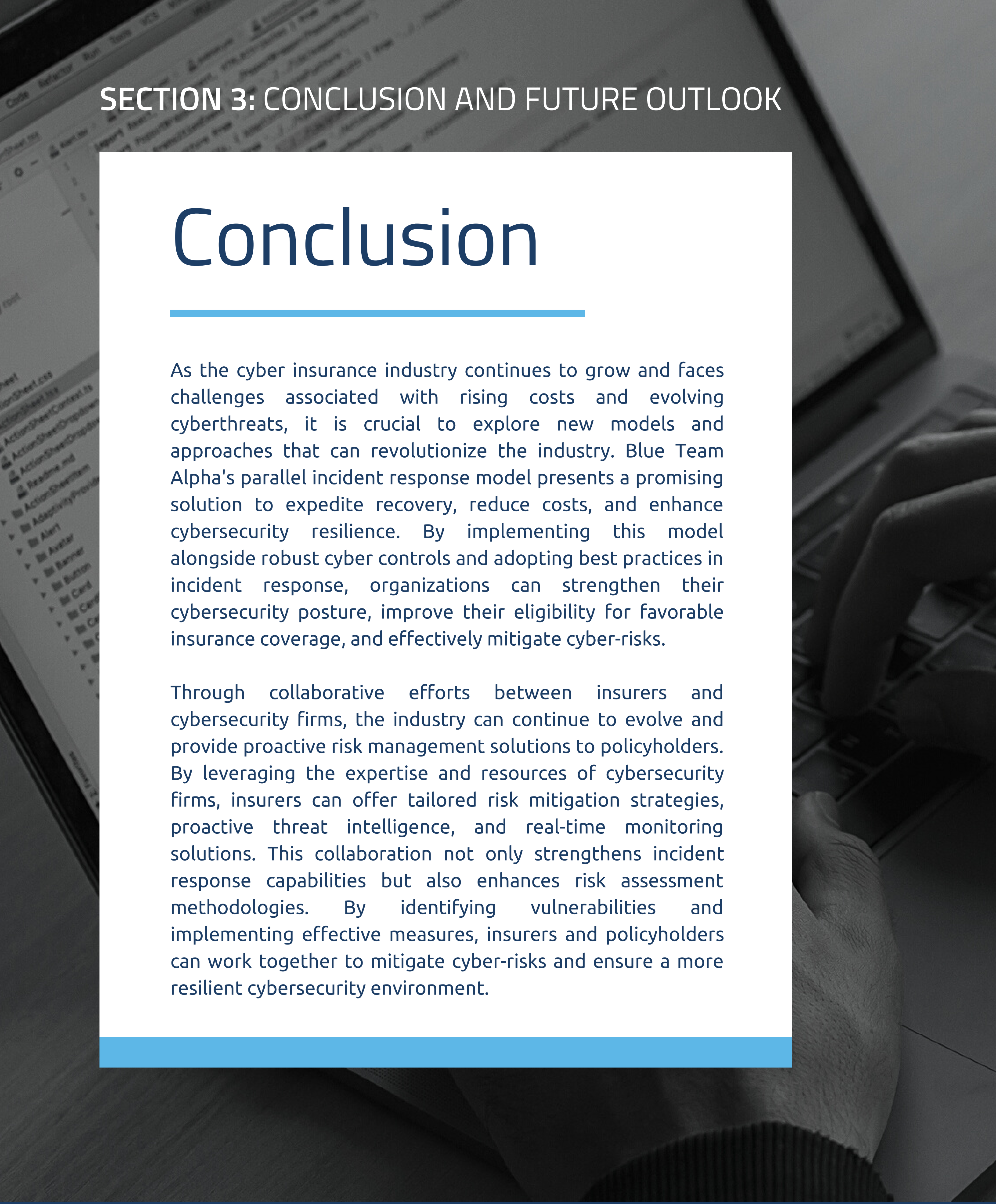
Recognizing the limitations of the current incident response model in the face of increasing cyberthreats, Blue Team Alpha proposes a new approach that operates in parallel rather than serially. This parallel model aims to minimize downtime, reduce damage, and decrease the overall cost of cyber breaches. By addressing incident response steps concurrently, Blue Team Alpha expedites the recovery process and minimizes the impact of cyber breaches. With their expert staff and comprehensive skill set, they can handle all aspects of a cyberattack, including forensics, response coordination, and post-incident recovery. By adopting this parallel model, Blue Team Alpha not only restores clients to operational status in an average of three to five days but also ensures that the organization emerges from the incident with increased resilience and improved security posture. This alternative approach has significant implications for cyber insurance claims as well.

Implications for Claims and Coverage

The limitations of the current incident response model have necessitated exploring alternative approaches to cyber insurance claims. Blue Team Alpha's parallel incident response model offers a promising solution by addressing the shortcomings of the traditional serial model. By operating in parallel rather than serially, the parallel model enables faster recovery, reduced costs, and enhanced cybersecurity resilience. Organizations striving to mitigate cyber risks and secure adequate insurance coverage can benefit significantly from adopting a parallel incident response approach.

The current incident response model's limitations have necessitated exploring alternative approaches to cyber insurance claims. Blue Team Alpha's parallel incident response model offers a promising solution by addressing the shortcomings of the serial model, enabling faster recovery, reduced costs, and enhanced cybersecurity resilience. As organizations strive to mitigate cyber-risks and secure adequate insurance coverage, adopting a parallel incident response approach can yield significant benefits. By embracing this model, organizations can strengthen their incident response capabilities, improve their overall security posture, and increase their eligibility for favorable cyber insurance terms.

Insurers work with policyholders to identify vulnerabilities and implement measures to mitigate cyber-risk. This includes providing guidance on best practices for cybersecurity, regular assessments, and offering resources for cybersecurity training and awareness programs for employees. By actively managing cyber-risk, organizations can reduce the likelihood of a successful cyberattack and lower their insurance premiums.



SECTION 3: CONCLUSION AND FUTURE OUTLOOK

Conclusion

As the cyber insurance industry continues to grow and faces challenges associated with rising costs and evolving cyberthreats, it is crucial to explore new models and approaches that can revolutionize the industry. Blue Team Alpha's parallel incident response model presents a promising solution to expedite recovery, reduce costs, and enhance cybersecurity resilience. By implementing this model alongside robust cyber controls and adopting best practices in incident response, organizations can strengthen their cybersecurity posture, improve their eligibility for favorable insurance coverage, and effectively mitigate cyber-risks.

Through collaborative efforts between insurers and cybersecurity firms, the industry can continue to evolve and provide proactive risk management solutions to policyholders. By leveraging the expertise and resources of cybersecurity firms, insurers can offer tailored risk mitigation strategies, proactive threat intelligence, and real-time monitoring solutions. This collaboration not only strengthens incident response capabilities but also enhances risk assessment methodologies. By identifying vulnerabilities and implementing effective measures, insurers and policyholders can work together to mitigate cyber-risks and ensure a more resilient cybersecurity environment.

Outlook

The cyber insurance industry is expected to further adapt to the changing landscape of cyberthreats. Continued collaboration between insurers and cybersecurity firms will play a critical role in developing innovative solutions to meet the evolving needs of policyholders. By staying proactive and embracing emerging technologies and practices, the industry can offer comprehensive risk management solutions that go beyond traditional insurance coverage.

Furthermore, as organizations strive to enhance their cybersecurity posture, investing in ongoing cybersecurity training and awareness programs is essential. By continuously improving their cybersecurity hygiene, organizations can reduce the likelihood of successful cyberattacks and improve their eligibility for favorable insurance terms. The cyber insurance industry will continue to emphasize the importance of solid cyber controls and incident response capabilities, rewarding organizations that demonstrate a commitment to robust cybersecurity practices.

In conclusion, by adopting new models and approaches, such as Blue Team Alpha's parallel incident response model, and collaborating with cybersecurity firms, the cyber insurance industry can revolutionize its practices and provide policyholders with proactive risk management solutions. The industry's continuous evolution will help organizations effectively mitigate cyber-risks, strengthen their cybersecurity resilience, and secure appropriate insurance coverage in an increasingly complex and dynamic threat landscape.

Sources

1. Researchandmarkets.com. (n.d.). Global Cyber Insurance Market - Forecasts from 2022 to 2027. Retrieved from https://www.researchandmarkets.com/reports/5746780/global-cyber-insurance-market-forecasts-from-2022-to-2027
2. NetDiligence. (2022). NETDILIGENCE® CYBER CLAIMS STUDY 2022 REPORT NetD_2022_Claims_Study_1.0_PUBLIC.pdf. Retrieved from https://netdiligence.com/wp-content/uploads/2022/02/NetD_2022_Claims_Study_1.0_PUBLIC.pdf
3. Woodruff Sawyer. (2022). Cyber liability: Looking ahead to 2022. Retrieved from https://woodruffsawyer.com/wp-content/uploads/2022/01/Cyber-Looking%20Ahead-Guide-2022_Web.pdf
4. Quinn, J., & Krauss, J. D. (2022). Cyber liability 2022 year in review and look ahead to 2023. Willis Towers Watson. Retrieved from https://www.wtwco.com/en-us/insights/2022/12/cyber-liability-2022-year-in-review-and-look-ahead-to-2023
5. Security.org. (2021). Cyber insurance statistics and data for 2023. Retrieved from https://www.security.org/insurance/cyber/statistics/
6. Woodruff Sawyer. (2021). Critical cyber security controls for insurance renewals. Retrieved from https://woodruffsawyer.com/cyber-liability/critical-cyber-security-controls-insurance-renewal/
7. Minimum Requirements in Cyber Insurance. Retrieved from https://www.cyberinsuranceacademy.com/knowledge-hub/guide/cyber-insurance-minimum-requirements/.
8. Cyber Insurance: Policies, Coverage, Requirements & More. Retrieved from https://www.cynet.com/blog/cyber-insurance-for-the-digital-era-what-it-is-and-who-needs-it/.
9. The 9 Cyber Insurance Requirements You Need to Know | tenfold. Retrieved from https://www.tenfold-security.com/en/cyber-insurance/.
10. Meet Cyber Insurance Requirements and Reduce Risk | CyberArk. Retrieved from https://www.cyberark.com/cyber-insurance/.
11. Cyber Insurance | Federal Trade Commission. Retrieved from https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance.
12. Report on the Cybersecurity Insurance Market - National Association of Insurance Commissioners (NAIC). Retrieved from https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf.
13. Cyber Insurance Market Overview: Fourth Quarter 2021 - Marsh. Retrieved from https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html.
14. Overview - Cyber Insurance Academy. Retrieved from https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf.