CERIAS
The Center for Education and Research in Information Assurance and Security

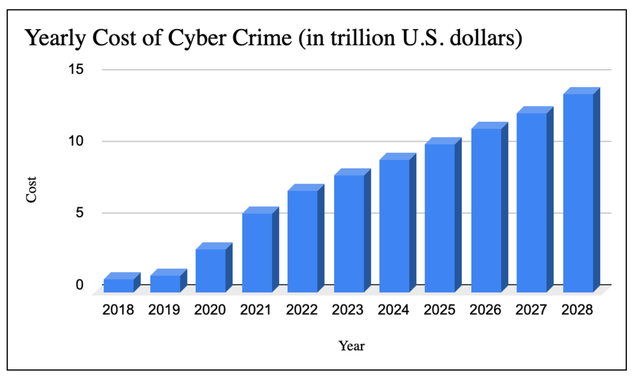
Securing the Future: A strategic framework for Cyber Liability Insurance

Janith D'Alwis | jdalwis@purdue.edu | jdalwis.com

Abstract: With cybercrimes predicted to cost the world $10.5 trillion in 2025, this cyber liability framework is a crucial blueprint for businesses navigating the ever changing digital landscape. As cybercrime continues to become more sophisticated the financial repercussions for unprepared entities surge, underscoring the indispensable role of cyber liability insurance. This research delineates a comprehensive insurance framework tailored to mitigate financial losses, safeguard digital assets, and ensure business continuity. By incorporating a meticulous risk assessment, customized coverage options, and promoting cybersecurity best practices, the proposed framework addresses the multifaceted nature of cyber risks. This research provides a strategic pathway for businesses to shield themselves against the burgeoning financial and operational impacts of cyber threats, thereby securing their future in an increasingly digitized global landscape.

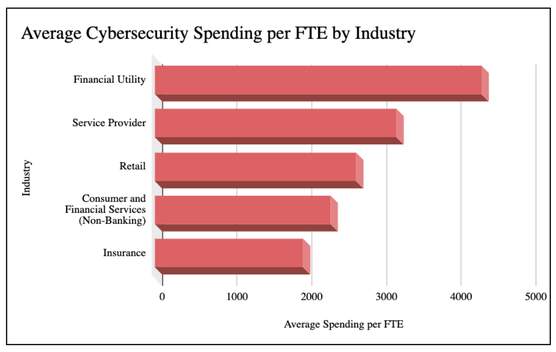
Featured Application: This research aids organizations in adopting cyber liability insurance and strategically navigating the cybercrime landscape, guiding budget allocation and financial planning to enhance cybersecurity measures and ensure business continuity.

Keywords: Advanced Persistent Threats (APTs), Denial of Service (DoS), Full Time Employee (FTE), Small to Mid-Sized Businesses (SMBs), Identity and Access Management (IAM), Attack Surface, Penetration Testing, Access Control, Protected Health Information (PHI)



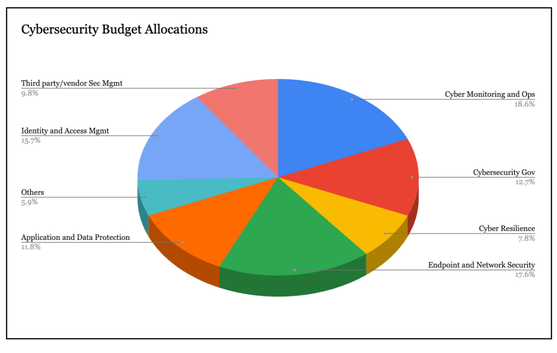
When the pandemic forced businesses to migrate to remote work environments, larger attack surfaces and security gaps became heavily exploited by bad actors. This surge worsened with the onset of advancements in AI and machine learning, which have significantly lowered the barrier for executing sophisticated cyberattacks. These technological leaps not only enhance legitimate industries but also offer cybercriminals tools to automate attacks, making them more frequent, complex, and difficult to detect. Additionally, some APTs have evolved to the point where they operate with their own organizational structures and departments, further professionalizing cybercrime and enhancing their ability to target businesses globally.

Understanding the landscape of cybersecurity expenditure illuminates critical insights into the vulnerabilities and priorities of businesses across industries. As of recent data, the technology, healthcare, and business services sectors stand out as the frontrunners in terms of cyber spending. These industries are inherently high risk due to the material sensitivity and potential rewards for bad actors. This allocation underscores the recognition of the inherent risks and the necessity to fortify digital assets against cyber threats within these industries.

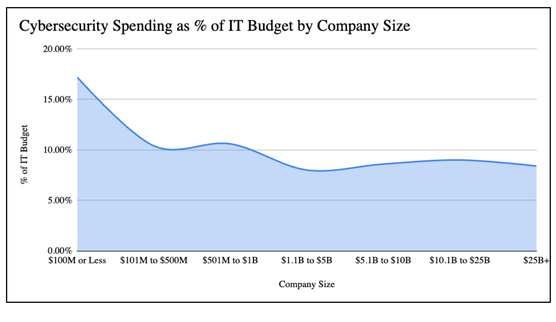


On average, approximately 9.9% of IT budgets are earmarked for cybersecurity measures. However, an intriguing trend emerges concerning the correlation between a company's size and its allocation of IT spending toward cybersecurity. Larger companies tend to allocate a smaller percentage of their IT budgets to cybersecurity compared to smaller counterparts. This phenomenon suggests either a discrepancy in risk perception or a belief in the resilience of their existing security measures among larger corporations.

Nevertheless, the disproportionate impact of cyber attacks on SMBs cannot be understated. Despite smaller allocations for cybersecurity, these entities often bear the brunt of cyber incidents. The average cost of a data breach for SMBs stands at a staggering $3 million, a figure significantly higher than the overall average cost of $4.45 million for companies across all sizes. Additionally, the average ransomware attack inflicts a financial toll of approximately $740,000 on SMBs, further exacerbating their vulnerability to financial strain and operational disruptions.

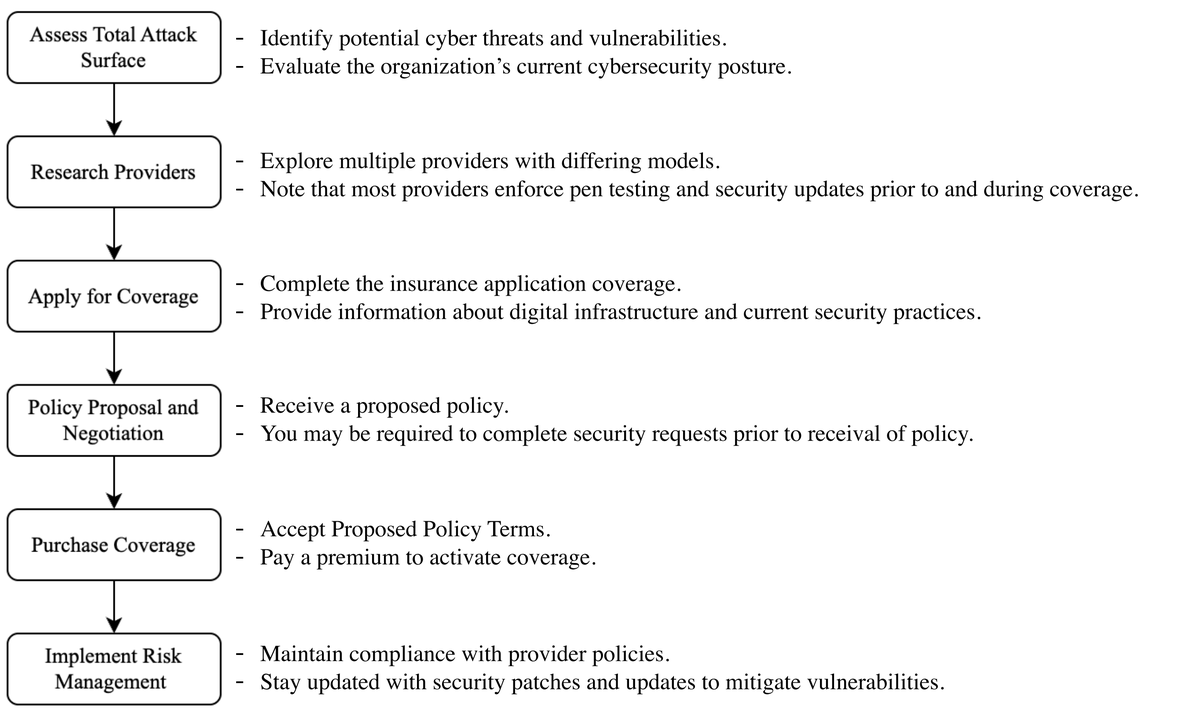


The disparity in the impact of cyber attacks on SMBs can be attributed to several factors. Firstly, limited resources and expertise hinder their ability to implement robust cybersecurity measures, rendering them more susceptible to exploitation by cybercriminals. Furthermore, the financial repercussions of cyber incidents, such as regulatory fines, legal fees, and reputational damage, pose existential threats to the viability of SMBs.



In light of these realities, the projected increase in cybersecurity spending from $168.8 billion in 2023 to an anticipated $192.2 billion in 2024 illustrates the escalating urgency to mitigate cyber risks and safeguard digital assets. This upward trajectory reflects a growing recognition of the evolving cyber threat landscape and the imperative for proactive investment in cybersecurity measures to protect businesses of all sizes against cybercrime.

When approaching Cyber Liability Insurance, an organization may follow a similar path as described below. Throughout the process it's vital that a coverage that best fits business needs and budget constraints is adopted. Finally, it should be remembered that Cyber Liability Insurance is NOT an alternative to comprehensive Risk Management, Incident Response, and Access Control but rather a supplement.

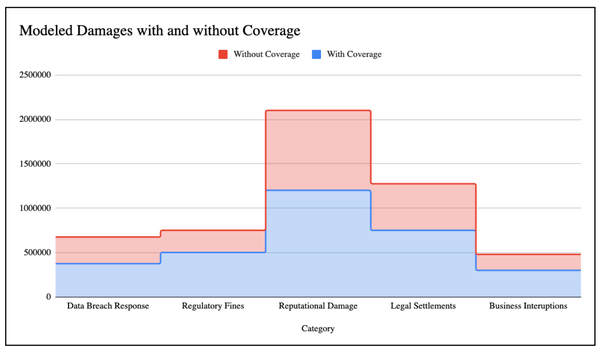


Real World Cyber Claims from Insurance Provider Chubbs

Risk	Industry	Business
Loss of PHI	***Healthcare***	***Commercial***
Payment Card Scam	Restaurant/Hospitality	Commercial
ATM Skimming	Financial Institutions	Commercial
Business Interruption	Retail	Commercial

A healthcare organization was informed by law enforcement that its patients' information was found on the dark web. It is believed that criminals from outside the U.S. were able to exploit vulnerabilities in the Insured's system to access more than 200,000 patients' PHI (personal health information). Chubb assisted the Insured by retaining an incident response coach and a forensics firm from our cyber panel. Several governmental/regulatory agencies were notified with the assistance of the coach. A call center was established and credit monitoring was offered to the affected patients.

- Cyber Claims Scenarios for Healthcare Organizations



Summary

Cybercrime rates are soaring, with projections estimating a global cost of $10.5 trillion by 2025, driven by technological advancements like AI and machine learning, which have made sophisticated cyberattacks more accessible. Cybercriminals now operate with organized structures, heightening the complexity and frequency of attacks. Certain sectors, including technology, healthcare, and business services, are prioritizing cybersecurity spending due to their inherent vulnerability. Despite this, larger companies allocate a smaller proportion of their IT budgets to cybersecurity compared to smaller ones. Small and medium-sized businesses (SMBs) face disproportionate impacts from cyber incidents due to limited resources and expertise, with the average cost of a data breach reaching $3 million for SMBs. To counteract these threats, global spending on cybersecurity is expected to rise from $168.8 billion in 2023 to $192.2 billion in 2024, highlighting the growing urgency to fortify digital defenses against cybercrime.

Cyber liability insurance plays a crucial role in helping organizations mitigate the financial risks associated with cybercrime. As cyber threats continue to evolve and pose significant challenges to businesses of all sizes, cyber insurance offers a safety net by providing coverage for various aspects of cyber incidents. This type of insurance typically covers expenses related to data breaches, including forensic investigations, legal fees, notification costs, and even extortion payments in the case of ransomware attacks. Moreover, cyber liability insurance can assist in managing reputational damage by funding public relations efforts and offering crisis management support. Importantly, it serves as a proactive measure to complement existing cybersecurity measures, providing organizations with peace of mind knowing they have financial protection in the event of a cyber incident.

As cyber threats become increasingly sophisticated and costly, cyber liability insurance emerges as a critical component of comprehensive risk management strategies, enabling businesses to safeguard their operations and assets against the ever-present threat of cybercriminals.

References

Chubb. (n.d.). *Cyber Insurance Claims Scenarios & Examples*. Chubb. https://www.chubb.com/us-en/business-insurance/products/cyber-insurance/cyber-insurance-claims-scenarios.html

Deloitte. (n.d.-a). *Reshaping the cybersecurity landscape*. Deloitte. https://www2.deloitte.com/content/dam/insights/us/articles/6507_Cybersecurity-FS-ISAC/DI_2020-FS-ISAC-Cybersecurity.pdf

Delinea. (n.d.). *Closing the cyber insurance gap*. Delinea. https://delinea.com/hubfs/Delinea/whitepapers/delinea-wp-2023-state-of-cyber-insurance-report.pdf

Reed, C. (2024, January 7). *Cost of Cybersecurity & Cybercrime*. Firewall Times. https://firewalltimes.com/cost-of-cybersecurity-cybercrime/

Ghosh, I. (2019, October 28). *Visualizing the massive cost of Cybercrime*. Visual Capitalist. https://www.visualcapitalist.com/cybercrime-costs/#google_vignette

Fleck, A., & Richter, F. (2024, February 22). *Infographic: Cybercrime expected to skyrocket in coming years*. Statista Daily Data. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Morgan, S. (2021, April 27). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

PURDUE UNIVERSITY

CERIAS