Analyze the author’s evidence of the unique challenges with cyber risk and discuss whether you agree with his assessment of the relationship between the availability of historical data and cybersecurity insurance.

Dekorte presents compelling evidence highlighting the unique challenges associated with cyber risks, which significantly impact insurance companies' ability to offer coverage for the cybersecurity industry. He emphasizes that the evolving legal and regulatory landscape of cybersecurity contributes to the uncertainty surrounding cyber insurance coverage. For instance, the legal cases of Medidata Solutions Inc. vs. Federal Insurance Co. and American Tooling Center, Inc. vs. Travelers Casualty, involving fraudulent fund transfers via email, exemplify the inconsistencies in the interpretation of policy language and the definition of insurance coverage. This lack of clarity in policy development and inconsistencies in guiding laws can lead to disputes and litigation.

Furthermore, the technological complexity associated with cyber risk poses challenges. Multinational companies like Google and Microsoft utilize millions of lines of code, making insurance applications for these companies complex and exposing them to a vast and intricate landscape of potential vulnerabilities. The ever-evolving threat landscape, including sophisticated tools like botnets and machine learning, makes it difficult to defend against emerging threats. Additionally, the interconnected nature of computer networks and the internet exposes companies' assets to cyber attackers, leading to widespread losses that can potentially overwhelm insurers or the entire industry. Hence, this lack of data increases the difficulty of quantifying and managing accumulation risk.

The availability of historical data on cyber incidents is crucial for insurers to effectively price cybersecurity insurance. Data is necessary for formulating pricing models, analyzing risk, estimating potential losses, and understanding the frequency and severity of past events to identify patterns and trends. However, organizations are often reluctant to disclose information about cyberattacks due to concerns about reputational damage, legal liability, and the potential for future attacks. This reluctance makes it difficult for insurers to apply their frameworks and actuarial approaches to cyber risk assessment and pricing. The dynamic nature of cyber risk, including the evolution of technology and the constant emergence of new threats and vulnerabilities, poses a serious threat to reliance on historical data, as it may not be predictive of future losses. This underscores the need for dynamic risk assessment and modeling techniques that can adapt to the evolving cyber landscape.

While a lack of historical data can impede the development of robust cyber insurance, other factors, such as the complex nature of cybersecurity, the evolving nature of cyberattacks, and market conditions, also contribute significantly to the challenges faced by the insurance industry in formulating models for the cyber industry. The availability of comprehensive and historical data on cyber incidents is crucial for developing a mature and effective cyber insurance market. Factors like market competition, reinsurance costs, and economic conditions can also influence the pricing model for cyber insurance.

References

Dekorte, R. (2019). Cybersecurity Insurance: Toward a more effective marketplace (Master's project capstone, Utica College). ProQuest.