The Public Company Cybersecurity Act

Nelson Tate

***Abstract*— This paper gives three perspectives on the proposed Public Company Cybersecurity Act (PCCA). We first describe the viewpoint in favor of PCCA, before moving onto the opposing viewpoint. Lastly, the views of the author are considered.**

***Index Terms*—cybersecurity, PCCA, regulation, economic growth**

I. SUPPORTING PCCA

The Public Company Cybersecurity Act (PCCA) aims to take the requirements for financial institutions in New York implemented by the New York State Department of Financial Services (NYDFS) and apply them to all publicly traded companies regulated by the SEC. In today's world, cybersecurity is an ever-evolving threat. In 2023 alone, 97% of organizations reported to have experienced an increase in cyber threats [1]. With the always increasing frequency in attacks on companies, it is important to make sure that all companies have ways to protect themselves. PCCA will lead companies towards a future of better cybersecurity through improved standards, investor confidence, and market growth.

PCCA aims to help companies defend themselves in many ways by increasing their cybersecurity. It aims to improve the standards for cybersecurity across all companies. Multi-factor authentication is one of the best ways to help a company prepare itself; another thing a company must do for itself is hire a Chief Information Security Officer (CISO) who reports to the board annually [2]. The position of CISO continues to change as the world of cybersecurity and business changes. Originally meant to target cybersecurity, this position has evolved to focus on other areas such as privacy, strategy, and network infrastructure [3]. By branching out to these areas, CISOs will be able to better handle a company's cybersecurity.

Another benefit of PCCA is increased investor confidence. Investors are constantly concerned with the cybersecurity of the companies that they have money invested in. The estimated yearly cost of cybercrime and cybersecurity globally in 2025 is around $10.5 trillion [4]. Section 500.17 of PCCA would mandate that companies report a cyberattack within 72 hours. If they make a payment on the ransom, they are required to notify the payment within 24 hours [5]. Adding rules such as these promotes transparency with investors demonstrating a company's initiative in the improvement of its cybersecurity.

Lastly, PCCA will benefit the market over the long run. Cyberattacks cause disruptions in all areas, but especially in the economy. Losses for cybercrime in 2023 were reported to be around $12.5 billion [6]. This number continues to grow every year as more and more cyberattacks are committed. PCCA reduces the risk of attack and loss through the promotion of incident response and recovery plans. Section 500.16 mandates that very company has a business continuity and disaster recovery (BCDR) plan that will allow them to get back into operation as swiftly as possible, ensuring that none of their data or their shareholders data has been compromised [7]. This also allows companies to recover any critical data that may be lost by just going to a backup of their operations, a much better alternative to paying off the cyber attackers.

PCCA will continue to improve the stability of the cybersecurity world. Companies will be able to have leadership in their CISO, their investors will be more confident, and the market will see even more growth under these rules.

II. OPPOSING PCCA

While PCCA may seem very beneficial to many companies and can help create more secure digital infrastructure, there are many flaws also associated with it: a one-size fits all approach, overregulation, and increasing compliance costs are all possible negative side effects of PCCA.

Cyber threats are constantly evolving, and one thing that is needed to combat them are laws and regulations. However, in its current form, PCCA is designed to be a one-size-fits-all approach that applies the NYDFS's regulations on financial institutions to all publicly traded companies. Due to this approach, every company needs to hire a CISO as mentioned above. The hiring process of a CISO may be too expensive or challenging for smaller companies compared to larger ones. PCCA also does not account for industry-specific risks. For example, a technology company and an apparel company do not need to have the same controls in place to operate successfully. A one-size-fits-all approach does not give companies the ability to target their specific problems and needs [8]. While these requirements may work for one company, another may have gaps in its security due to PCCA's regulations.

One of PCCA's biggest issues is the number of strict rules that are imposed on all companies. The risk of

overregulation and overlapping of rules is very high due to the nature of PCCA. Many companies already follow industry-specific frameworks, which may already have clauses like PCCA. This overlap may cause companies to view PCCA as redundant and possible confusing. The biggest risk of overregulation is that of confusion and inefficiency [9]. As more and more rules are from both federal and state governments, companies will have to implement and follow them. This increases the time, effort, and cost that companies spend on training preventing them from performing their actual jobs [10]. One possible negative of overregulation is driving companies out of the market. If a smaller company cannot afford to comply with PCCA, it may decide to leave the market or go to an international market with less regulations.

Implementing PCCA may result in considerable compliance costs for companies, especially smaller firms with access to fewer resources. PCCA would require companies to establish risk assessments, annual employee training, and perform penetration testing [11]. While these are important for companies, smaller ones may struggle to keep up with these rules due to their scale. They may have to pour more resources towards these rules, preventing them from seeing economic growth.

III. RECCOMENDATION

After looking at the arguments both for and against PCCA, there are many aspects of it that are not best suited for a lot of businesses. It is my recommendation that we do not pass PCCA in its current state.

Due to the one-size-fits-all approach, many smaller companies may face increased pressure to comply with PCCA. While it would benefit them to meet the rules, they may not be able to afford the extra requirements. Because no industry is the same, PCCA may also be better tailored towards industries with higher risk, such as tech or financial services; however, other lower risk industries may not need as many regulations to be just as secure. Instead, PCCA should allow industry-based regulations.

In conclusion, while the intentions of PCCA are for the better interest of all companies and cybersecurity, there are amendments that can be made to prevent overlap and improve cybersecurity and economic growth. Senator Moderate should consider voting against PCCA until the revisions have been made.

REFERENCES

[1] “Cyber Resilient Business | Accenture,” www.accenture.com. https://www.accenture.com/us-en/insights/cyber-security-index

[2] “NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES SECOND AMENDMENT TO 23 NYCRR 500 CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES.” Available: https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf

[3] “2024 Deloitte-NASCIO Cybersecurity Study,” Deloitte Insights, Sep. 29, 2024. https://www2.deloitte.com/us/en/insights/industry/public-sector/2024-deloitte-nascio-cybersecurity-study.html?id=us:2ps:3gl:nascio24:eng:gps:011025:ciso%20role:e:c:kwd-456562806210&gad_source=1&gclid=CjwKCAiAh6y9BhBREiwApBLHC813e1DUyLn7ibh2mqH_3dQRvF85SUQZk4aZW_5GeNEBv5rVLJEYoxoCA18QAvD_BwE (accessed Feb. 11, 2025).

[4] Cybersecurity Consulting Services & Strategies | Accenture, “Accenture | Security Solutions,” Accenture.com, 2025. https://www.accenture.com/us-en/services/cybersecurity?c=acn_glb_semcapabilitiesgoogle_14206874&n=psgs_0924&&&&&gad_source=1&gclid=CjwKCAiAh6y9BhBREiwApBLHC5pRviZiVP9P2gW416lrmWTNbzS-Lw3e7tF-nhaOQbBbwuMPTggM3RoCtb4QAvD_BwE&gclsrc=aw.ds (accessed Feb. 11, 2025).

[5] “NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES SECOND AMENDMENT TO 23 NYCRR 500 CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES.” Available: https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf

[6] F. Zandt, “Infographic: How Much Money Is Lost to Cybercrime?,” Statista Daily Data, May 31, 2024. https://www.statista.com/chart/32341/worldwide-reported-losses-connected-to-cybercrime/

[7] “NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES SECOND AMENDMENT TO 23 NYCRR 500 CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES.” Available: https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf

[8] J. Rende, “Why A One-Size-Fits-All ‘Compliance’ Plan Can Be Dangerous,” Forbes, Oct. 13, 2023. Available: https://www.forbes.com/councils/forbestechcouncil/2023/10/13/why-a-one-size-fits-all-compliance-plan-can-be-dangerous/

[9] [1]R. Jan, “Navigating Over-Regulation In Cybersecurity,” Forbes, Dec. 09, 2024. Available: https://www.forbes.com/councils/forbestechcouncil/2024/12/09/navigating-over-regulation-in-cybersecurity/

[10] [1]V. Gisladottir, A. A. Ganin, J. M. Keisler, J. Kepner, and I. Linkov, “Resilience of Cyber Systems with Over- and Underregulation,” Risk Analysis, vol. 37, no. 9, pp. 1644–1651, Dec. 2016, doi: https://doi.org/10.1111/risa.12729.

[11] “NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES SECOND AMENDMENT TO 23 NYCRR 500 CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES.” Available: https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf