Sahil Khanna
CS 3710
02/02/2023
Word Count: 483

## How to Fortify US Cybersecurity Policy

Educating lawmakers on cybersecurity would be a big step in improving cybersecurity standards in the US. Currently, representatives are not technology oriented and are unable to understand the need for cybersecurity. They are thus inclined to allocate funding for other issues. Making both state and federal lawmakers participate in a cybersecurity education program would make cybersecurity legislation easier to pass. For example, cybersecurity issues would be able to receive appropriate funding once legislators understand the requirement for this funding.

The effect of this would not just be limited to better cybersecurity legislation. More funding for cybersecurity programs would also attract more knowledgeable individuals to join as government cybersecurity jobs will be more financially competitive. Having government employees also reduces the issue of outsourcing cybersecurity to third-party organizations, helping prevent possible leaks due to individuals with access to classified information who either have malicious intentions or are careless. Thus, the impact of increased funding toward cybersecurity through educating legislators about the issue will be significant. An example of this is a recent bill to increase the amount of cybersecurity legislation that received bipartisan support.[1] Legislators are working to create a $10 million fund to increase cybersecurity education so that more cybersecurity professionals can enter the workforce and US cybersecurity can be strengthened. With an increase in legislator education at both the state and federal levels, more such funding can be expected to be approved soon.

A second measure to make cybersecurity in the US more robust is to use Artificial Intelligence for cybersecurity purposes. AI can be used to identify and locate vulnerabilities in systems. Using AI to scan government websites, systems, and technologies can help the government patch up these vulnerabilities before they are attacked. Since the US government usually has slow responses to cybersecurity issues due to a small staff, knowing of these vulnerabilities in advance can help them work to fix them before they become apparent to potential threats. Doing this at a state and federal level can upgrade the strength of government systems in the US.

While this is being applied very minimally today in government agencies, if it were to be applied, the benefits would be immense. This can be seen in the rapid rise of cybersecurity companies that use AI. Crowdstrike, an AI-driven cybersecurity company, recorded a financial year revenue of $2.34 Billion till October 2022.[2]  The fact that big corporations are using these cybersecurity companies to fortify their cyber defense points to the effectiveness of this method.

1.  Gross, Grant. "House Cybersecurity Education Funding Bill Draws Bipartisan Support." Restmethod. oring America , Restoring America , 11 Nov. 2022, https://www.washingtonexaminer.com/restoring-america/courage-strength-optimism/house-cybersecurity-education-funding-bipartisan-support.
2.  CrowdStrike Financial Report 2022: https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-third-quarter-fiscal-year-2023-financial#:~:text=Annual%20Recurring%20Revenue%20(ARR)%20increased,ARR%20added%20in%20the%20quarter

Though it will not completely fix all cybersecurity issues in the US, by implementing these two suggestions, I believe that big strides can be made in the overall strength of US cybersecurity. Effective cybersecurity policies and methods can be put in place which would reduce data breaches and hacks. These are important changes to be made as cyber warfare becomes more prevalent on an international scale.

1. Gross, Grant. "House Cybersecurity Education Funding Bill Draws Bipartisan Support." Restmethod. oring America , Restoring America , 11 Nov. 2022, https://www.washingtonexaminer.com/restoring-america/courage-strength-optimism/house-cybersecurity-education-funding-bipartisan-support.
2. CrowdStrike Financial Report 2022: https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-third-quarter-fiscal-year-2023-financial#:~:text=Annual%20Recurring%20Revenue%20(ARR)%20increased,ARR%20added%20in%20the%20quarter