SEC votes to propose new rules for cybersecurity disclosure and incident reporting [UPDATED]

Written by Cooley LLP

This article discusses about how business has not allocated resources on cybersecurity. The current Covid-19 pandemic situation has changed dynamics on cybersecurity. There is a massive number of people working from home which caused more threats globally affecting businesses and within the cybersecurity realm. Article also discusses more about how threats have gone up, some more severe but also mention how cybersecurity sometimes would not be a good idea because of wrong timing for companies. It has been hard to find people who are willing invest on companies on behalf of cybersecurity. There is also an issue of threats not being reported at all. The government SEC has set policies for companies to follow sensible decisions to make investors aware of cybersecurity and how to take action on cybersecurity risks within their companies. SEC describes step-wise method on how to deal with cyber attacks. First step SEC issue as a guideline is cyber threats reporting. Second step is opening up about cybersecurity and about cybersecurity risks on how to tackle them. Investors want to know how companies respond to cybersecurity threats and what kind of mitigations can be applied to stop them. The SEC chair is willing to support the bill that (if passed by senate and house) would allow investors to study the cybersecurity measures to be put in place within their companies with regards to cybersecurity threats that are not being reported. This article can be applied to day to day security but many of us do not take cybersecurity seriously enough. When we are on social media or browsing through the internet, when we open many different kinds of emails day to day we are liable suffer security threats knowingly or unknowingly. We are not concerned so much about cyber threats in general unless if the hacker or person does commit harm to us directly when we are online. This article describes how giant corporations or small businesses happen to be not reporting cybersecurity threats at all. This is because no investors available at all in some cases or there are not many companies who are willing spend money on it. This has effected globally since start on of pandemic as more and more people started working from home causing an increase cyber threats. Some of the deficiencies that this article has is that it does not mention details on why not many investors care about cybersecurity and why within company's incident reporting system itself that they the incidents and not being reported. It's also an unanswered question why investors are not available in this sector who are willing step up support to organization or small business on this matter. I do agree with this article to a certain extent but I think investors and shareholders need more understanding on cybersecurity in order for them to step up investing on cybersecurity to protect their vulnerable systems and assets within their organizations or businesses. I also see this being a problem into the future if more and more pandemics start to escalate. There has to be a way to prepare themselves from being compromised with cyberattacks and there has to be things to be in place to protect organizations ranging from large corporations to small businesses. We need to find more ways to invest in cyber security and more has to be done throughout this sector .in regards to cyber incidents not being reported. There has to be division or a body within the organization or business, overlooking threats and sealing off vulnerable areas so that the bad actors will not be able

to get into them. We need to be aware as people on cyber threats in the world when it comes to financial data within organization or a business. There has to ways to be put in place protective and effective firewalls so that we can protect company assets in business. There has to be also more investments in cyber security since there are so many bad actors and many cyber criminals are everywhere. Cybersecurity should be prioritized in every business and every organization not just when the organization gets into cyber attack but before even before event is likely to happen.