# Cyber attack awareness in the article: unlike chess, everyone cust continue playi...

Technology, Information Technology

This article was wrote by Michael Clark and Charles E. Harrell. Michael Clark is SpecialCounsel and Charles E. Harrell is a Partner, both based at Duane Morris LLP, Houston, Texas, USA. The motive of this paper is to familiarize readers about the nature and extent of the risks that listed companies and their boards of directors' face by not addressing their attention to insuring the cyber-security of their operations and not disclosing cyber-episodes and their impact on operations as suggested by the SEC's Division of Corporate Finance.

This article examined issues related to cyber-incidents in light of the heightened importance for publicly-traded companies to install and maintain adequate procedures and controls for safeguarding private information—along with their potential liability if they fail to do so. Other than that the introduction briefly explained about cases on cyber security and cyber law that was being issued in US, the government of United States of America acknowledge this attacks and brought to attention by authorities and even the president himself which was president Obama at the time.

It issued that cyber-attacks have been growing year by year but the government cyber security infrastructure has not change thus leading to massive loss in term of money to repair the damage made by the cyber-attacks. Because of the issues being brought up the government came up with polices to encounter this kind of attacks to defend himself from being breach, as it stated 102 successful attacks per week have been recorded meaning that they have to do something to prevent the numbers from multiplying.

This article mainly investigate issues related to cyber-incidents. In relation with Malaysia cyber-attacks occurrences are not similar with US as the attacks in Malaysia are limited or slightly. According to The Star newspaper cyber-attacks in Malaysia reported at least 12 cases in the year of 2017. Compared to US our cases are not classified as major threats but also being taken care of to prevent anything from damaging our government's information or data. Recently this year Malaysia was shocked upon a news published by The Sun Daily stated that Malaysia once again faced cyber-attack but this time it may cost our economy 12. 2 US$ due to cyber security incidents which was handled by the authorities and the statement they told to the reporters were " We need to be ready to face this and find ways to lower the risks". With the US providing policies, Malaysian government has also implemented a few cyber law to help prevent any cyber-attacks from happening. The latest policy implemented was on 2010 which is Personal Data Protection Act 2010.

## Benefits

As in the article the author stated that cyber-attacks brought attention to the government which then led to awareness. Relating this to Malaysian government, reported of cyber-attacks can help build a counter to prevent it from happening again thus producing awareness to people about cyber-attacks and cyber law provided by the government. This helps people to be more aware of the business or personal data because of action taken from this issue.

Other than giving awareness cyber security can prevent government official’s website from going down. According to the article cyber-attack tend to focus government data or investment companies, which is commonly being hosted by their own sources. With cyber security approach it can help these website from shutting down which will cost a huge amount of loss if it were to shut down for recovery. Cyber security provides layer of security to prevent it from being attack from unknown threats.

Next, by identifying cyber-attacks according to the article the Malaysian government can produce new policy to help solve new problem or threat. It can also strengthen old policy to become more efficient and reliable to serve and protect data from being attack by anonymous source. A strong policy can help in each aspects because the aim is to protect organization or individual as long as it is being followed by the people.

Furthermore, the article explained how cyber-attacks effects companies with financial business nature for instance investment agencies. Cyber security implemented by Malaysian government can improve stakeholder confidence in your information security arrangements and improved company credentials with the correct security controls in place thus leads to the increase of economy and improve future business for the nation.

## Implications

The author mainly focused on the cyber-attacks towards government agencies or organization but individual logically without cyber security, cyber-attacks can damage individuals in term of theft of information, theft of

financial information for instance bank details or payment details, theft of money and disruption to trading example inability to carry out transactions online. With cyber law or cyber security it helps individual protect general safety and ensure the rights as users of the cyber world. Cyber security also helps people with secure browsing that is safe from spyware or any related of its kind thus preventing any damage that can be done towards an individual.

Cyber-attacks differ from people and agencies because the commonly cyber-attacks on people are usually scamming, phishing or theft of financial data meanwhile for agencies cyber-attacks aim to steal corporate data or information relating to their business of work. Cyber-attack on people suffer a bit more if using the problem in the article because the article stated any problem regarding to cyber-attack the government will take actions upon it mean while cyber-attack on people are usually handled by non-government agency or self-handled, either way it does not fully resolve the problem because of the lack of attention and power.

Meanwhile cyber security on nation is a massive impact in terms of economy or the nation defense. Nation also have to face the possibility of a terrorist attack that uses cyber methods or uses the combined powers of physical and cyber-attacks to achieve the goal of an operation. This is where cyber security comes handy because it can prevent from this traumatic event from occurring. Nation cyber security can bolster national cyber capabilities and develop resilient information infrastructure run by an educated national workforce. Governments would also benefit from developing an international

information exchange, early warning and assistance mechanisms for swift reaction in times of crisis, as well as establishing a consultation framework with other countries, this approach are manipulated from what the article mentioned.

Recommendation

The government should lead in launching a high-profile national approach to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs. Government administration should focus on, and recommend, long-term authorization and sufficient appropriations for, high-quality, effective cybersecurity education and workforce development programs in its budget proposals in order to grow and sustain the cybersecurity workforce.

Private and public sectors need to transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce by emphasizing and expanding opportunities for retraining so that current employees as well as displaced workers and veterans can be reskilled to take on cybersecurity roles. Other than that educate and train users, this may sound normal but with the proper education and training government user can be more aware and cope the surrounding of cyber security thus can dealt with the problem from bursting. Back up data, although cyber security provide protection but in this world even protected sources can be breached and data might be stolen. By backing up data it can provide a copy that can help from data loss.

## Solution

According to the article the solution stated made logically sense in my opinion which is providing a proper cyber security with the latest information needed. This can be implemented in any country as it will help to encounter cyber-attacks or at least manage to handle it for the time being. Implementing policies can also dealt with cyber threat as it provide strategy to overcome the cyber-attack. According to the parliament of Singapore, one of the advance country in Asia, some of the cyber-attack cannot be dealt with because lack of cyber-security. But government has an option to move on and leave it be or propose a way to resolve the cyber-attack which usual forming a new cyber-security or implementing new policy to overcome the damage that have been done and prevent it from happening again in the future.

Some countries overcome cyber-attacks by forming a a highly skilled professionals with the purpose of providing the best defence to protect data from being breach or stolen. Malaysia however dealt cyber-attacks with the help of agencies such as MCMC and Cyber Security Malaysia, providing consultation and protection for national data as well as monitoring the access of certain information by users. This method prepares them for any negative outcome from happening and spreading awareness towards government or society upon any cyber-attack.

## Conclusion

In conclusion this article provide adequate knowledge upon cyber-attack and cyber security and bring awareness towards readers on the stated subject. It

also gives me a new perspective upon cyber security and how important it is to manage in order to protect the nation’s information or personal information. It also explained the damages that can be done if cyber security is not well implemented in any country. How it can affect the stability of economy and the military defence of any nation, it also gives a bigger picture on how cyber security works to protect and prevent from any unwanted threats or cyber-attacks.

Furthermore Cyber security is equally important for local, state, and central government as these organizations maintain a huge amount of confidential data and records concerning the country and its citizens. Yet several government organizations face difficulty in protecting data because of inadequate secured infrastructure, limited funding and lack of security awareness. Stealing of confidential data or sensitive information, digital by terrorists from government organizations, as well as digital spying can lead to serious threats on a country. For this reason, cyber security is of paramount importance for government organizations also and is a vital asset to the nation.

# Reference:

1. 1. Clark, M., & Harrell, C. E. (2013, 11). Unlike chess, everyone must continue playing after a cyber-attack. Journal of Investment Compliance, 14(4), 5-12. doi: 10. 1108/joic-10-2013-00342