NOTE FOR NATIONAL DEFENCE:
Cyber-Security Vulnerabilities and Protection Against Cyber Incidents

Authors: Saman Asvadi[1] and Mohsen Farhadloo[2]
[1] Graduate student, John Molson School of Business, Concordia University, Montreal, Canada
[2] Professor, John Molson School of Business, Concordia University, Montreal, Canada

SUMMARY

- Cybercrime is any kind of crime, involving a computer or a network of computers. Computers may be either used to attack or be attacked by criminals. In such category of crimes, information of a person, a business or even an organization is theft by the criminals. Malicious use of this information endangers personal, organizational or even public security or financial health [1].
- According to a recent survey conducted by Allianz in 2019 [2], cyber incidents pose the grates amount of risk to businesses and organizations, forming 37% of global risks to them. Based on this survey, cybercrimes result in an average $600 billion per year. They also mention that the number of cybercrimes, and finical loses due to them are growing exponentially.
- The same research indicates that, cyber incidents is the cause of business and organizational interruption in 50% of the cases [2].
- A business may not breakdown only due to cyber-attacks to itself, but any cyber-attacks to its suppliers as well, can breakdown the operations in the core business [3]. It is highly recommended that a business consciously assesses its suppliers' security risk, and help its suppliers, if need be, in case of cyber security, to boost its operations and reduce the risk of breakdown and loss of information.

CONTEXT

- Cyber Security Risks:

  - ❑ London's Strategic Dialogue Center highlights the risk that terrorist groups may engage in cyber war, as the technological infrastructure to commit such attacks are not costly and highly available. These groups may invest to train members on the technological knowledge to commit such crimes.
  - ❑ Mike Rogers, former director of the US National Security Agency, mentioned that cyber warfare and threat is very much common, happening every day around the globe [3].
  - ❑ One recent example of the effect of cyber threat and warfare is the Syrian and Ukrainian crisis.

- Cyberattacks can destroy huge databases owned by the government, containing data about citizens, secure issues and so forth. These attacks also can disrupt infrastructures like energy and nuclear infrastructures. Such attacks, not only cause huge financial loses, but also endanger the life of people.
- European Network and Data Security Agency (ENISA) mentions that most cyber security incidents are not reported [4]. This avoidance in reporting, hinders deep research on the source of these attaches, research on the weaknesses of IT infrastructures and lack of knowledge of the users. For the time being, it is not clear whether the main weakness against cyber-attacks is the lack of knowledge of the users or insufficiently secure IT infrastructure.
- In many cases, it is even impossible to locate where the attackers are located and who did such an attack.
- Law makers should consider cybercrimes and research on them more comprehensively, to set proper laws to hinder attackers as much as possible and punish them.
- As studied by the Center of Strategic International Studies in the United States, most cyber attackers are in Russia, Vietnam, Brazil, North Korea, and Indi, while China is the most active country in cyber spying [6].

RECOMMENDATIONS

- In this section some recommendations are made to improve IT infrastructures against cyber-attacks. As proposed in [3], there is a need to redefine strategies and infrastructures to prevent against cyberattacks and minimize the damage of such attacks. It should be kept in mind that, it is not possible to redesign the infrastructure, but it is for sure possible to boost existing ones.
- Since the issue of cyberattacks is a worldwide concern, and a person, company or organization may be attacked from outside the borders, it is inevitable to cooperate with other countries and nations, to boost cyber security.
- It is suggested that law makers establish new cyber law and regulations and update them on a routine, to try to minimize the number of cyberattacks. It goes beyond saying that Law makers need the collaboration of police and governments to efficiently apply the rules and regulations they make. Moreover, law makers need to be up to date about most recent cybercrimes.
- Work force in governmental organizations, ministry of defence, and any other business or organization dealing with sensitive data, should be trained about cyber security and how hinder attackers.
- A safe protocol and technology should be considered and used to transfer sensitive information from police to jurisdictive organizations and vice versa.
- Nations should plan to educate their citizens to be aware of cyberattacks and their outcomes, and proactively defend against such attacks and to take proper security measures into consideration [3].
- Support services institutes should be established, so that when people are attacked, they can call such institutes, seek advice, and ask for help if necessary [3].
- Governments should consider a protocol for reporting cyberattacks and inform the public about it. They must encourage all people, businesses, and organizations that envisage cyberattacks to report the attack promptly. Hence, researchers can better investigate cybercrimes, and can better suggest policies to boost IT infrastructures against such crimes.

References

[1] https://en.wikipedia.org/wiki/Cybercrime
[2] Corporate, A. G. (2019). Speciality: Allianz Risk Barometer: Top Business Risks for 2019. *Munich, Germany*.
[3] Čelik, P. (2019). Institutional Measures for Increasing the Cyber Security for Business in the European Union. *Economic Themes*, *57*(3), 351-364.
[4] cyber-Europe 2018: after action report. https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report
[5] Cyber-Europe 2012 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2012
[6] McAfee, N. L. (2014). Estimating the global cost of cybercrime, economic impact of cybercrime ii. *Center for Strategic and International Studies*.