MOBILIZING INSIGHTS IN DEFENCE AND SECURITY
MINDS
MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Security-Policy NET Nexus of Emerging Technologies

BRIFING NOTE FOR Department of National Defence
Security Issues Related to the Use of Information Technology (IT)

Saman Asvadi [1] and Mohsen Farhadloo [2]
[1] PhD candidate, John Molson School of Business, Concordia University, Montreal, Canada
[2] Professor, John Molson School of Business, Concordia University, Montreal, Canada.

SUMMARY

- Hackers target users of systems more often than the vulnerabilities in the system, since attacking through human element is way too much easier than dedicating time to find vulnerabilities in a system. [2]
- Organizations must put the right employee at the right position, and male sure that he/she is aware of the security issues regarding the systems he/she uses [1]
- A survey conducted in [1] indicates that there is a high correlation between awareness and security. The more the employees are aware of security problems that may arise when they are working, and how to deal with them, the less the number of security attacks and hackings are.

CONTEXT

- People are the first point of defence in cyber security. As a result, it is highly essential to assess and improve their awareness about cyber risks and treads, as well as training them about ways to prevent cyber risks, and ways to deal with security risks.[2]
- Even the most sere and sophisticated technologies can be easily hacked by hackers, if they can trick the users. That is, if the user is not enough aware of the security risks and the ways to avoid them. [3]
- The technology that is being used in an enterprise or an organization must be up to date and user friendly. Each user of the technology must be trained about cyber security, based on his/her role in the organization, and the information he/she has access to. [1]

- If the employees are continuously trained and assessed about cyber security, and the managers complement them in this process, organizations can eliminate cyber security risks , or at least mitigate their effect. [4]
- The survey conducted in [1] reveals that, the higher the position of an employee in the organization is, the more the employee is aware of physical security. In their survey 49.6% of the entry level employees, 50.03% in intermediate positions, 54% of the middle level managers, and 53.6% of higher managers were sufficiently aware about cyber security, cyber treats, and ways to avoid them.
- The results of the survey in [1] also indicated that, the higher the level of the employee in the organization is, the higher is the physical security of the system the employee is working with.

RECOMMENDATIONS:

- Each organization has to establish cyber security measures, and implement them continuously, to avoid anyone with malicious reasons to have access to systems, data centers, locked server rooms, etc. [1]
- Each organization must have a cyber security committee, to define cyber security policies, and make sure that the employees are aware of these policies. Also, to make sure that these policies are consciously implemented and maintained. [1]
- It is suggested that, organizations assess the level of awareness of the employees, and based of this level assessment, and the needs of the organization, they can train the employees about cyber security issues.

REFERENCES:

[1] Dahbur, Kamal, Ziad Bashabsheh, and Deema Bashabsheh. "Assessment of security awareness: A qualitative and quantitative study." *International Management Review* 13.1 (2017): 37.

[2] Aloul, Fadi A. "The need for effective information security awareness." *Journal of advances in information technology* 3.3 (2012): 176-183.

[3] Spears, Janine L., and Henri Barki. "User participation in information systems security risk management." *MIS quarterly* (2010): 503-522.

[4] Conrad, E., Misenar, S., & Feldman, J.”*CISSP Study Guide.*Waltham,” MA, US Syngress Publishing. (2016)