REASONS FOR VULNERABILITY IN ORGANIZATIONAL SYSTEMS

There are several reasons why organizations get hacked, but generally speaking it is caused by carelessness and lack of proper security on the part of the organizations. The negative effect of hacking can be very scandalous, take for example the US election result, it was greatly affected due to the hacking of the email of the democrat candidate, we can also look into several hacking situations like the yahoo and the effect it has on the organization. Here are eight common causes of hacking:

- *It is caused sometimes as a result of failure to properly test code before it's been used.*
- *Lack of updated OS and making sure that it has valid support and are not expired. Also, systems in the organization should use secure antivirus. Most of these things are overlooked but they are very essential to the security of every organization.*
- *It can also be by leaving source code exposed. This should be protected as hackers find and utilize weakness.*
- *Failure to change passwords from the default settings is one very important reason why organizations get hacked. Organizations/firms should change their passwords regularly and use secure codes.*

- *The practice of poor patching strategy within an organization can leave it open to hacking.*
- *Phishing and human error in social engineering has been a huge issue for firms, as it exposes them to breach. They need to educate their users on how to recognize suspicious data and also protect their accounts properly.*
- *Poor monitoring of data leaving the organization. The destination of every outbound information should be properly investigated.*
- *Failure to recognize infiltration makes companies easy prey for cyber attackers. Good network segmentation is a key to better security.*

Abdulaziz AL-Humoud
Senior Security Engineer