International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Cyber Security - A Business Accelerator??

Riya V S[1], Dr. Aarthy C[2]

[1, 2]Department of BBA, PES University, Bangalore, India

1) South Korea attack 2013
2) Target Hack 2013
3) The German Steel Plant meltdown 2014
4) Tesco Bank 2016
5) Bangladesh Bank hack 2016
6) Dyn Cyberattack 2016

What is the common thread running amongst the above incidents?

If we delve deeper, you will find that all of the above have been victims of cyberattacks that have exploited vulnerabilities in the IT infrastructure.

IT has disrupted businesses over the past decade like no other technology has ever. As IT increasingly touches our lives in many different ways like internet banking, online shopping, smart homes and self-driven cars, our dependency on IT is reaching a point of no return. Information Security (InfoSec)/Security in the Digital Economy is practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information (Wikipedia). It is the series of measures deployed by organizations to ensure that their customer data and business critical information are accessed and consumed by authorized people only. InfoSec also ensures that the above mentioned information is not altered or erased inadvertently. It can be leveraged by business to securely expand and be global. So, it is imperative that information security be at the forefront of all organizations to ensure there is secure delivery of services to customers, and the privacy of citizens is protected. It is equally important that the assets of an organization are protected against cyberattacks.

Why should a business secure its IT assets? As most companies these days use online channel for their financial transactions. Hackers can compromise on IT system and gain unauthorized access to sensitive information like customer credentials, account details etc. A company may lose its valuable research data to competitors who can sabotage the information to create inhospitable competition in the market for competitive advantage, money, hacktivity and/or personal gain. Countries critical installations like power grids, nuclear power generation plants, military installations can be brought down by the terrorists through systems that are not secure and create a catastrophe in the society. Effective security to encounter cyber threat is a combination of best practices and technology. For example, even the best of burglar alarms will be ineffective if the security team does not investigate the cause for it to go off. Every business faces threat from cyberattacks, the solution for this problem is not to obscure but to effectively counter digital threats with the use of technologies and best practices. Some of the technologies that are commonly used for securing IT infrastructure are Antivirus, Firewall, Intrusion prevention system, Data encryption technologies, Secure Email gateways, Antimalware technologies.

The best practices recommended by industry experts from Cisco are, strong authentication and authorization mechanism. That is, to login to a system one must require an id and a password; the id is the identity of the user and the password is the authentication mechanism. Authorization on the other hand means specifying access rights and controls to a defined set of users to access only those resources that are allowed to them, right access is given to a user based on the roles and responsibilities he performs in an organization; for example, a salesperson will only be given sales resources but not HR or finance database. Securing remote access is another practice which creates a private tunnel connecting the remote users to the corporate resources ensuring the flow of data through the channel remains confidential and protected. This enables organizations to expand their business & allow employees, partners & customers to connect to them securely.

John Chambers, chairman of Cisco, famously said that there are only two types of companies in the world. Ones that have been hacked & the second ones that have been hacked but don't know of it yet. No organization can be declared 100% Secure in today's world & no amount of throwing technology at the problem will make it go away. All security technologies & practices should aim to increase the cost of an attack for an attacker. The best approach to Security is a layered one which has multiple deterrent mechanisms at different parts of the IT infrastructure; it is akin to having multiple doors, safes & locks to safeguard the family jewels at home.

The objective of any business is to be innovative and profitable. The approach to security has to be an all-inclusive one to include assets and processes of a business which might be IT or non IT. Information security in today's world plays a ubiquitous role in running a profitable enterprise. It is difficult to fathom a business without a well incorporated information security structure, therefore the saying 'Compromising on IT is a compromise on the business itself'. Thus, effective Security helps protect the organization from cyberattacks & also accelerate growth by leveraging technology to drive the business goals.