DEWAN P.N. CHOPRA & CO.

INTERNAL AUDIT UPDATE

Importance of Cyber Security in Current Times

Importance of Cyber Security in Current Times

The Covid-19 pandemic has brought about major changes in work culture. It is not just the business pressure caused by the uncertainty, at a fundamental level it has transformed the way we work. The change in the concept from office workplace to work from home has evolved so quickly that even the most traditional and technologically backward firms have had to adapt on to the need of the hour and accustom its practices according to the changing work culture.

If we weren't already familiar with video conferencing, team IM tools, and cloud-based file sharing before March last year, we are now. And only due to these technologies we could survive the world's largest pandemic.

Remote working has accelerated digital transformation across companies. Prior to the pandemic, the report states, only 5% of survey respondents worked from home most of the time, but now 87% of workers want the ability to choose where, how, and when they work

With these changes in the work environment there lie the data related risks. In the pre COVID-19 era, most employees worked from offices, where the local area network (LAN) as well as the desktops/laptops were adequately secured. Sophisticated technologies could protect against cyberattacks that originated primarily from the internet and targeted the enterprise network. Enterprise protection technologies secure the employees' systems from targeted phishing campaigns that lure them into clicking on unknown links and attachments.

In covid-19 pandemic major challenges to deal with cyber security breaches were:

1. The wireless routers are a shared asset with the family, neighbors and visitors. If the data connection is unsecured then the data traffic flow is not controlled and covers all sorts of data search including personal email and educational needs, social media activity.
2. A corporate user on the home network can access unfiltered internet, personal email and drives unlike in the past, where the user was governed by the IT security team and is now a COVID-19 specific phishing theme target.
3. A home user clicking on an unsuspecting link or redirected to a malicious website could end up loading malicious codes into the browser of the corporate user's laptop which gets executed unsuspectingly in the background and proceeds to compromise the enterprise network.

   Earlier Offices offered an additional layer of security in the sense that employees can check in with their colleague in the neighboring cubicle or their manager and alert the IT security team if they notice any suspicious emails or links.

4. The malicious code could also extract valid corporate credentials when the home user would log into the enterprise portal or VPN via keylogging or tab-nabbing, thereby compromising the security of the entire organization.
5. There are also heightened risks of IP theft and leakages, especially for work-from-home users operating for organizations.
6. Phishing incidents rose 220 per cent during the height of the Covid-19 pandemic compared to the yearly average, a new report by F5 Labs reveals. Covid-19 – related phishing emails mainly manifested themselves as fraudulent donations to fake charities, credential harvesting and malware delivery.

7. In 2020 to date, 52 per cent of phishing sites have used target brand names and identities in their website addresses. As per the reports Amazon was the most targeted brand in the second half of 2020. Paypal, Apple, WhatsApp, Microsoft Office, Netflix, and Instagram were also among the top ten most impersonated brands.

Technology has come as an aid to survive the world's largest pandemic. Therefore, it is equally important for an institution and organization to prevent the threats imposed by technology by putting a strong and unbreakable cyber security in place.