INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY
(Established by Reserve Bank of India)

Explore, Enable, Excel

IDRBT WEBINAR SERIES FOR BOARD DIRECTORS

Webinar No: 2 **Topic: Cyber Security: During Covid and Beyond**

Date: June 12, 2020 **Speaker: R. Gandhi,** Former Deputy Governor, Reserve Bank of India

KEY TAKEAWAYS

A. Because of COVID, there has been and will be fundamental shifts in beliefs, attitudes and behaviours. The Banking and financial sector, with its heavy reliance on technology and digitalization, could leverage that capability.

B. But several adhoc decisions and measures had to be resorted to. The need for speed and expediency dictated such decisions and measures. Several known risks became "acceptable", which during normal times were clearly "not acceptable".

C. During the lockdown, technology systems were put to test at unprecedented levels. Cyber threats including phishing attacks and also sophisticated ones like malware, trojan attacks, ransomewares, etc., increased. There was also an increase in money laundering and terrorist financing risks stemming from Covid-19-related crimes.

D. Remote working tools / software like video conferencing software were target of attacks. Sensitive data travelled along with game, music, TV content, Alexa, etc. Malicious COVID based emails increased. Remote onboarding and remote identity verification brought in embedded risks.

E. As we move towards resuming normal activities, banks and financial institutions will have to make major changes to their structure, operations and approach.

F. First of all, they have to pay greater attention on crisis preparedness, systems resilience, and access to healthcare.

G. Secondly, banks will have to make structural changes in terms of being:

- Flexible – COVID dispelled the myth that banking being customer-oriented industry is not suitable for WFH. Banks will now have to let staff work from home. Rules, procedures, infrastructure, compensation etc., will need review and reassessment
- Redesigning Office layouts – Banks need to consider employee wellbeing more holistically - in terms of not only the physical, but also mental and emotional wellbeing. Redesigning the office layout to take care of social distancing (between staff and also between staff and customers), commitment to hygiene, cleanliness and safety, provisions for temperature checks, remodelling conference rooms, video rooms, etc., will be needed to be completed on an urgent basis.
- Helping staff redesign their homes and make them "work ready" – As many homes are not equipped for WFH, employees will need to be assisted in helping them build "office pods" at home with enduring cyber connectivity and security features.

H. Thirdly, the new mantra will be “working securely, while working remotely”. Banks will have to pay special attention for cyber security while enabling their staff to work remotely from home or on mobile spots.

I. Fourthly, banks will have to revisit their Business Continuity Plans (BCP). COVID has compelled us to revisit certain BCP assumptions, like, “people can reach/ airdash backup centres”. In such events of pandemic proportions, organisations will not be able to reach its staff to the Data Centres. Hence, WFH will be an integral part of BCP. Banks will have to quickly reorganise their data centres from “Active-Passive” centres to “Active-Active” centres.

J. Banks will have to identify succession planning in much greater granularity - second, third lines for every function have to be get ready. Revamping backup centre will have to include not just its infrastructure, capacity, and licenses; employee safety which was never on BCP radar will now become an important element of BCP.

K. Another area for special attention will be the third party services and providers availability; banks need to get a high degree of assurance in this regard, including system audit certification. Further, the current BCP locations have not been designed for extended period of operations; typically the recovery time objectives are within a day and if at all a couple of days. COVID Pandemic has taught us that alternate locations may have to be on full function basis for even three to six months. This has enormous implications for the BCP infrastructure redesigning.

L. Fifthly, banks will now have to take cyber security to a new orbit. With increasing reliance on digitalisation, banking has already been a fertile ground for hackers and cyber fraudsters, both organised and unorganised genre. With the virtual certainty of remote working and WFH being the new normal, the relevance and continued vigil on cyber security cannot be overemphasized. End-to-end communication safety standards will need continuous enhancements. Lastly, a strong element of cyber security will be to imbibe the security culture and security by design in the minds of every staff member.

****