

Bank CSIRT Launched To Ensure Information Security In Banking And Finance



Bank CSIRT (Computer Security Incident Response Team), a sector based task force for the prevention of cyber attacks on information systems of the banking and finance sector was launched with the auspices of Lalith Weeratunga, Secretary to the President. The Bank CSIRT website was also launched at the occasion with Lalith Weeratunga sending out the first Informational Alert to member banks.

Spearheaded by Sri Lanka Computer Emergency Readiness Team | Coordination Centre (CERT|CC), this critical innovative service is hosted and managed by LankaClear under the guidance of the Central Bank of Sri Lanka and the support of the Sri Lankan Banks Association (SLBA).

The importance of information security (IS) in the banking industry has grown exponentially over the past few years due to a combination of factors, such as regulatory requirements mandating information protection, the growth of

electronic banking and the increasing number of individuals and third parties with access to enterprise data. Hence, the establishment of a formal collaboration between financial institutions to pool critical information and knowledge is imperative to form greater synergies in fighting cyber threats and attacks.

Security is a dynamic process. Attacks against systems are evolving, as hackers and fraudsters continuously identify new ways to break through corporate security shields. Thus, the most important part of an information security programme is implementing processes to continuously assess security risks in order to allow them to respond as quickly as possible with stronger controls if necessary.

Lalith Weeratunga delivering the keynote address at the occasion said, “To my mind, this is one of the most important and timely initiatives we have taken in the modern age of IT and banking. The way we are connected today, we have opened many new avenues for people to attack. Invasion of our information systems happens on a daily basis. Many years ago, if an attack was carried out on an information system, it was easily located because there were not many Internet or IT users. But today this is extremely complex with the current connectivity.”

Further adding, he said, “There are times when Sri Lanka particularly is in focus. Then we see a number of phishing attacks. But the Sri Lanka CERT has been up to it and has been able to protect our information systems and I am very happy that the Information and Communication Technology Agency has made this organization very viable. And they have fought to protect the country’s information systems, away from the public eye.”

Lal Dias, CEO - Sri Lanka CERT|CC commenting on the initiative said, “Bank CSIRT will be one of the many sector-specific, CSIRTs established under the umbrella of Sri Lanka’s National CERT. The formation of a centralised trusted body to handle information security related incidents in the banking and finance sector will undoubtedly help address most of the sector specific issues. Additionally, the knowledge gained by resolving an incident at one particular bank can be utilised to resolve other affected banks issues and enable the issuance of early warnings and alerts in order that the banks can take preventive measures. Bank CSIRT can also disseminate information received from international Computer Emergency Response Teams (CERTs/CSIRTs) relating to new cyber security threats enabling individual banks and financial institutions to

take proactive action.