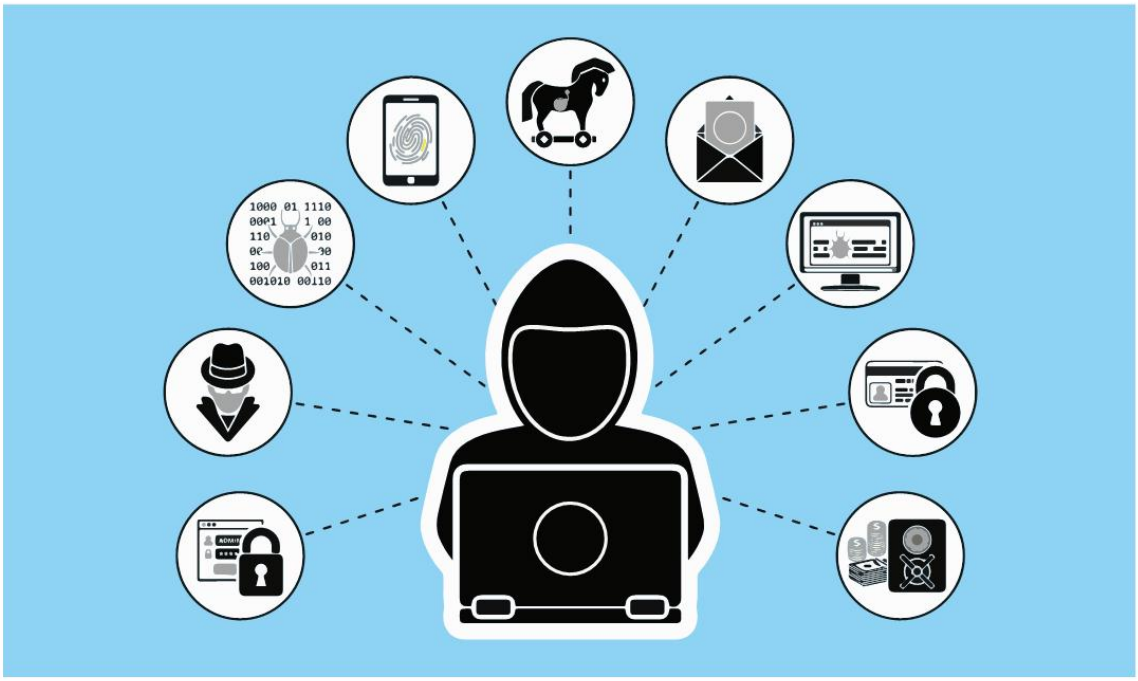
CEO INSIGHTS

RECENT TRENDS ON CYBER SECURITY

By Devendra Kumar Vyas, CEO, SREI Equipment Finance Ltd

SREI Equipment Finance Ltd. (SEFL) has emerged as one the major equipment financiers in India. The company enjoys a Pan-India presence with offices in 89 locations. SEFL has an experienced management team having significant expertise in the financial services.

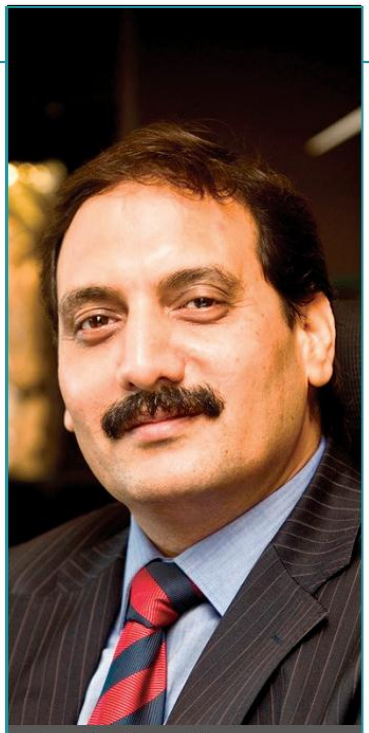
We as humans have increasingly sought connectivity with our fellow beings. During this journey, we ended up with one of the most amazing yet complex creation of mankind, the web. Be it inter or intra, today it's impossible to imagine a world without 'net'. The web (or net) has provided unprecedented connectivity and has the world communicating in real time. Today web provides connectivity to such a level that all the services, businesses, and every other possible model are available 'online'. Not only mass oriented services, but also business of niche institutions and very covert projects too, communicate on line. In a nutshell, today we are more dependent on the web than anything else. And with such dependence there is always the threat to the security; and in this case, cyber-security. Today no channel is cent percent secure. The Yahoo account breach, with around 500 million records hacked; the JP Morgan and Chase data



hack, affecting around 76 million households and numerous other hacks, are examples of ever increasing cyber – attacks.

What makes the situation worse is that banks and businesses are lagging in implementing defences against these hack threats. With new malware being deployed (more than 150,000 unique new strains each day); it is very difficult for the defences to keep pace. One of the challenges in defending against these attacks is the wide spectrum of attackers' profiles and vectors of the attacks. Organized crime circles are in this for financial gains, and espionage against governments and businesses. Some hackers do it just to create headlines. There is no defining division between players. It becomes difficult to classify them as the perpetrators are from different backgrounds. Organized crime rings are responsible for more than half of the attacks. State-affiliated entities are responsible for some attacks. Lone hackers, who are in it for either individual financial gain or the thrill of the chase, still initiate a small percentage of cyber-threats. Hackers such as Anonymous and Izz ad-Din al-Qassam Cyber Fighters (the group responsible for the high-profile and highly successful waves of DDoS attacks launched against U.S. FIs in September 2012) have certainly garnered plenty of headlines as a result of their attacks. Former and current employees are also an insidious threat.

Back home in India, these risks are being amplified by the increasing globalization of businesses and the booming market for IT services. Cyber Security should be an important parameter of businesses today. Along with the legal and financial aspects, considerations should be given on what is the acceptable levels cyber risk businesses can adopt. Publicity around a major business deal could also attract malicious activity as cyber criminals probe for weaknesses to exploit. On the positive side, Indian businesses are well aware of the security risks inherent in doing business today.



Devendra Kumar Vyas

> Within the IoT realm, more technology is evolving keeping the manufacturing and heavy engineering businesses in minds; and thus increasing the vulnerability of these businesses

Cyber Trends to Expect in the Short Term

- Credit card and information theft will be under more threat than ever, due to shifting of platforms to new payment technologies; like mobile wallets.
- In the light of recent attacks on the likes of cloud services of various vendors and other such examples; mainstream companies, especially which are consumer data heavy, will heavily adopt data, Data Theft Prevention practices.
- The Internet of Things is the next source of databases. Within the IoT realm, more technology is evolving keeping the manufacturing and heavy engineering businesses in minds; and thus increasing the vulnerability of these businesses, which should traditionally bereft of major data hacks.
- Mindset will shift to planning an effective response and recovery in an event of data breach, from trying to stop the breach from occurring.
- Business processes need to be designed with risk and compliance requirements integrated into their core for risk mitigation and transfer.
- For cost effectiveness, companies have been outsourcing important tasks to third parties, rather than developing them in-house. Very few have recognized the risks of outsourcing. Cyber/Net security will be accepted as part of an organization's ecosystem.

Top security priorities for the near future will be, continuous monitoring of systems, cloud computing security, mobile device security, and identity & access management, and regulatory compliances. There are huge economic losses occurring in the event of any cyber breach. Going forward we should see more indigenous security systems developed to mitigate the economic losses.