With increasing connectivity and the mass adoption of mobile devices, the threat to data has increased manyfold. As a result, global players are confronted by virus attacks and data breaches. In this context, Juniper Networks has identified six dominant modes of data breaches in 2012:

Simple attack methods on web applications remain effective: In the past year, many large public companies faced web application attacks like SQL injection and cross site scripting. These types of attacks continue to remain a popular hacking method because of their relatively low level of sophistication and the potential difficulty in detecting and preventing them.

Mobile malware and application-centric threats continue to pose a risk to enterprise data: With the continued adoption of “bring your own device” at the workplace, the risk of mobile malware and invasive applications impacting critical corporate data continues to be a prime concern. 2012 witnessed a significant increase in the number of malware and invasive applications aimed at mobile users. There was a 350 per cent increase in mobile malware between October 2011 and October 2012. The free applications are four times more likely to track a user’s location and three times more likely to access address books as compared to paid applications.

Increased transparency about data breaches: As the frequency of data breaches continues to increase, companies are being judged more on how they handle such incidents. Many companies are still not providing in-depth detail about the nature of a breach, but they are publicly acknowledging any such threats that they might have faced. This is an encouraging development in the industry as it will help raise awareness about the importance of securing data.

Botnets effectively controlled: Building on earlier success, public/private partnerships were successful in tackling several prominent botnets responsible for spam and other threats to data. Through a combination of forensic security research and legal arguments, researchers have been able to block the command and control systems of some of the most common botnets.

Sophisticated vulnerabilities related to NFC technology unveiled: One of the most interesting developments in the mobile security space is that several vulnerabilities related to the use of near field communication (NFC) technology have been revealed. 2012 marked an increase in NFC adoption, facilitated by the mass availability of applications related to finance and mobile wallet, which are based on the technology. Also, it has been proven to be an effective tool in demonstrating and tackling potential security hacks. In the past, security researchers have demonstrated the ease with which a device can be remotely controlled via NFC. While an actual attack is yet to occur on a NFC-based mobile application, the technology will remain a likely target as consumer adoption increases.

Advanced Attacks Targeting Government Infrastructure: While the existence of state-sponsored cyber-attacks and espionage on critical government and business systems has existed for years, 2012 saw a significant increase in sophisticated malware and other attacks. To counter such threats, a lot of countries like U.K. and Hong Kong are investing in new cyber-security capabilities.