Foreword

Reflecting on a very busy year for cyber security, I would like to highlight some key observations for 2012. No doubt, the increasing mobility of data in corporate environments is one of the biggest challenges we faced in the past year. Users are fully embracing the power to access data from anywhere. The rapid adoption of bring your own device (BYOD) and cloud are really accelerating this trend, and providing new vectors of attack.

Another trend we are seeing is the changing nature of the endpoint device, transforming organizations from a traditional homogeneous world of Windows systems to an environment of diverse platforms. Modern malware is effective at attacking new platforms and we are seeing rapid growth of malware targeting mobile devices. While malware for Android was just a lab example a few years ago, it has become a serious and growing threat.

BYOD is a rapidly evolving trend, and many of our customers and users actively embrace this trend. Employees are looking to use their smartphone, tablet, or next generation notebook to connect to corporate networks. That means IT departments are being asked to secure sensitive data on devices they have very little control over. BYOD can be a win-win for users and employers, but the security challenges are real while boundaries between business and private use are blurring. It raises questions on who owns, manages and secures devices and the data on them.

Finally, the web remains the dominant source of distribution for malware—in particular, malware using social engineering or targeting the browser and associated applications with exploits. For example, malware kits like Blackhole are a potent cocktail of a dozen or more exploits that target the tiniest security holes and take advantage of missing patches.

Cybercriminals tend to focus where the weak spots are and use a technique until it becomes less effective, and then move on to the next frontier. Security is at the heart of this revolution of BYOD and cloud. Protecting data in a world where systems are changing rapidly, and information flows freely, requires a coordinated ecosystem of security technologies at the endpoint, gateway, mobile devices and in the cloud.

IT security is evolving from a device-centric to a user-centric view, and the security requirements are many. A modern security strategy must focus on all the key components—enforcement of use policies, data encryption, secure access to corporate networks, productivity and content filtering, vulnerability and patch management, and of course threat and malware protection.

Best wishes,

Gerhard Eschelbeck CTO, Sophos