The Importance of Information Protection

Information is an important asset. To fully understand the importance of information security, there is need to appreciate both the value of information and the consequences of such information being compromised. The days when thieves would only steal laptops and desktops are long gone. Nowadays, thieves steal critical data and information contained in insurable hardware including mobile phones, giving rise to cyber-crime. The thieves are now called hackers.

Businesses will continue to hold sensitive information on their employees or customers, financial results and information that gives them a competitive edge such as trade secrets and business plans. As more and more of this information is stored and processed electronically, and transmitted across company networks or the internet, the risk of unauthorised access increases. Businesses are presented with the growing challenge of how best to protect this information, which if left unprotected, can be accessed by anyone leading to an information or security breach. When information falls into the wrong hands, it can ruin lives, bring businesses down and even be used to cause harm. It can also lead to huge financial penalties, expensive law suits, loss of reputation and business and can take years to recover from.

According to the Ponemon Institute and IBM 2016 data study where 350 companies from 11 companies were surveyed, the average total cost of a data breach for the participating companies increased 23% over the previous two years to $3.79 million. It was noted that the average cost paid for each lost or stolen record containing sensitive and confidential information increased 6%, jumping from $145 in 2015 to $154 in 2016. The lowest costs per lost or stolen record were in the transportation industry, at $121, and public sector, at $68. On the other hand, the retail industry's average cost increased dramatically, from $105 in 2015 to $165 in 2016.

What can a business do to protect itself from the growing risk of a security breach? As a first step to protecting its information assets, a business should undertake an Enterprise-wide Risk Assessment with an emphasis on Cyber Maturity Assessment (CMA) to identify its critical operations and flag areas of risk. For example, the assessment may point to poor vendor management where vendors have excessive and unsecure access to information assets. The business will then evaluate the measures it has in place to mitigate the risks identified. This exercise when conducted regularly will ensure that the systems and applications that process information in each area of operation are constantly reviewed and enhanced to meet the ever-evolving cyber risks.

Should a breach materialise and information assets are compromised, this then should immediately trigger an Incident Response (IR) plan. The IR plan would include: a forensic investigation; containing the attack by isolating the compromised assets; recovering systems to an operational level; and lastly continuous or regular monitoring of the entire environment. Most cyber insurance packages have a component of IR services.

Given the repercussions and cost of an information security breach to a business, information protection is not just desirable, it should be priority for management.
Having a clear means of identifying the risk or likelihood of a breach is important, mitigating this risk by proper insurance planning and having a response plan will bolster the company should such a breach occur.

Hamza Mzee
IT Services
KPMG Tanzania
hmzee@kpmg.co.tz
FOR MORE INFORMATION
www.kpmg.com/eastafrica