FREELANCE WRITING SAMPLES

SALES OPERATIONS

When Xerox first started a sales operations team in the 1970s, little did they anticipate the need and success of a sales operations team in the future. Xerox's aim was to have a dedicated team looking at analyzing data and providing insights to sales reps. Forty years later, the scope has broadened thanks to modern sales tools, evolving nature of the sales role, technological advancements and big data.

"Sales operations" means different things to different organizations but in a nutshell, sales operations aim to support and provide strategic direction to management and the sales team by providing them with analytics on current and future state and market intelligence data for key accounts which will help them sell in an efficient and effective manner with minimal hindrance.

SOFTWARE ASSET MANAGMENT

Software assets form the bedrock of an organization. An organization's duty does not end once they agree to the licensing term and pay a fee for the use of a software. Time and time again, we hear of cases where software vendors have sued companies for non-compliance of software assets. Like, SAP which is seeking US $600 million in compensation from Hoegaarden brewer Anheuser-Busch InBev, manufacturer of Budweiser and Stella Artois for breach of software license agreement.

Businesses are held accountable for the software assets they use throughout its lifecycle in the organization and because of this, more companies big and small are adopting Software Asset Management (SAM) process. SAM is a process by which companies can optimize the usage of their software assets and the deployment of software licenses to ensure compliance.

INFORMATION SECURITY MANAGMENT

"For every lock, there is someone out there trying to pick it or break in" - David Bernstein

Whitman and Mattord (2005) define information security management as, "the protection of information and its critical elements, including the systems and hardware that use, store and transmit information. Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure".

According to a study conducted by Forbes, 72% of respondents interviewed felt vulnerable to attacks. In an increasingly connected world, information is exposed to many vulnerabilities ranging from malicious code, virus attacks, ransomware threats and hacking. The history of security vulnerability can be first traced to the Morris Worm.

The Morris Worm was a maliciously program that was unleashed on the internet on November 2, 1988, from a computer at the Massachusetts Institute of Technology (MIT). The worm crippled 10% of the internet in less than 24 hours of infection, gathering widespread media attention. This attack was a wake-up call for governments to create policies for information security management, for developers to create cyber security measures and for companies to provide security services. The downside however was that it opened the floodgate for a whole new generation of hackers and creators of malicious content.