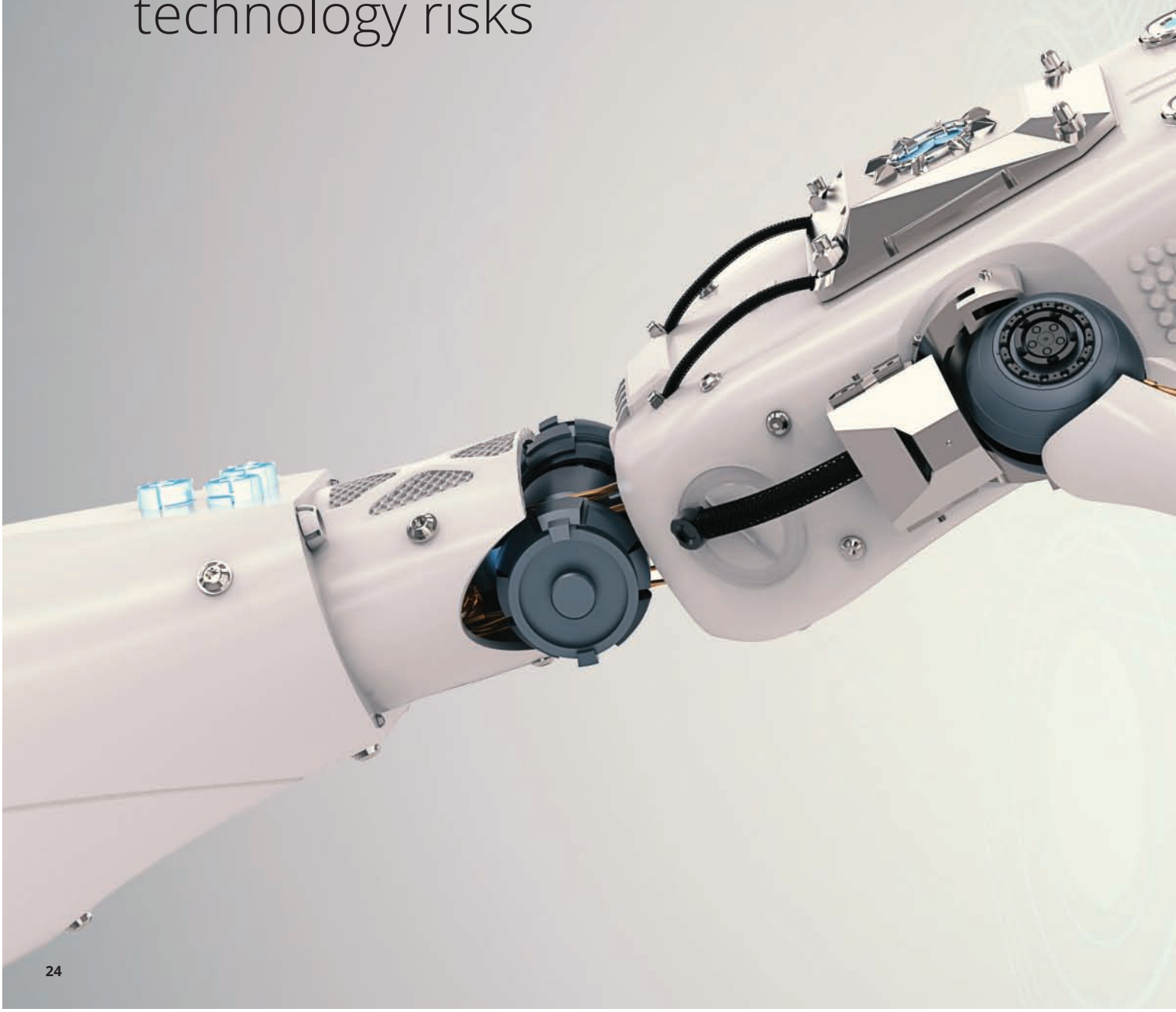
I am SAM

A strategic initiative to manage cyber and technology risks



Managing and maintaining software assets cannot be neglected, and it is also an overwhelming problem if not planned and executed effectively.

What is Software Asset Management (SAM)?

An effective asset management practice allows enterprises to integrate financial, contractual, and inventory functions to support their software and hardware asset management life-cycle and take strategic decisions to run their business. As such, managing software assets becomes an integral part of the Information Technology (IT) operations of any organization.

Software assets include items such as operating systems, applications, network management programs, enterprise resource planning (ERP) solutions, and other human resource (HR) and finance-related applications. Managing and maintaining software assets cannot be neglected, and it is also an overwhelming problem if not planned and executed effectively. Unaccounted-for software or applications within an enterprise could potentially introduce risks related to compliance, operational efficiencies, and security.

Key SAM risks

The key objectives of a SAM program are to:

- Provide an integrated and central view of all software deployed.
- Define a platform that enables the IT function to (re)assess its Software Lifecycle Management processes—that constitutes the procurement, usage and expiration of Enterprise Software assets.
- Assist the IT department to optimize its operational costs; and
- Manage the compliance, operational and information (or cyber) security risks related to the ownership and use of software.

Mitigating risks with SAM

Introducing and implementing a SAM program along with respective good practices can help an organization achieve the objectives outlined above and effectively mitigate and manage the risks related to compliance, operational efficiencies, and security. Some of these key risks are:

- Risks related to compliance:
  - The technology research and advisory firm Gartner, Inc. predicts an increase in vendor audits.[1] Companies may incur penalties in the event of a software license compliance audit if they do not keep their licenses organized and updated.
  - Risk of non-compliance with the specific terms and conditions within the software agreements with regards to the usage of software.
  - Select industries and geographies have regulatory compliance requirements related to SAM that the organization may be at risk of not complying with.
- Risks related to operational efficiencies:
  - Not being able to effectively monitor and track the software in use.
  - Organizations may be paying maintenance costs for software not being used.
  - Software licensing models and metrics are evolving with technology resulting

in rising complexities. Organizations face the risk of not being abreast with these changes, resulting in the risk of not using the most efficient and economical licensing model.
  - Re-allocation of software licenses when hardware is moved or decommissioned results in a software licensing impact.
- Risk related to security:
  - Without the ability to inventory and control software installed and allowed to run on their hardware, organizations make their systems more vulnerable to security threats.
  - Trends have indicated that backdoor malware or Trojans are primarily propagated through unauthorized software that is not accounted for or managed by the IT team.
  - Open source software, if not properly identified and controlled, could potentially introduce security risks to the organization.

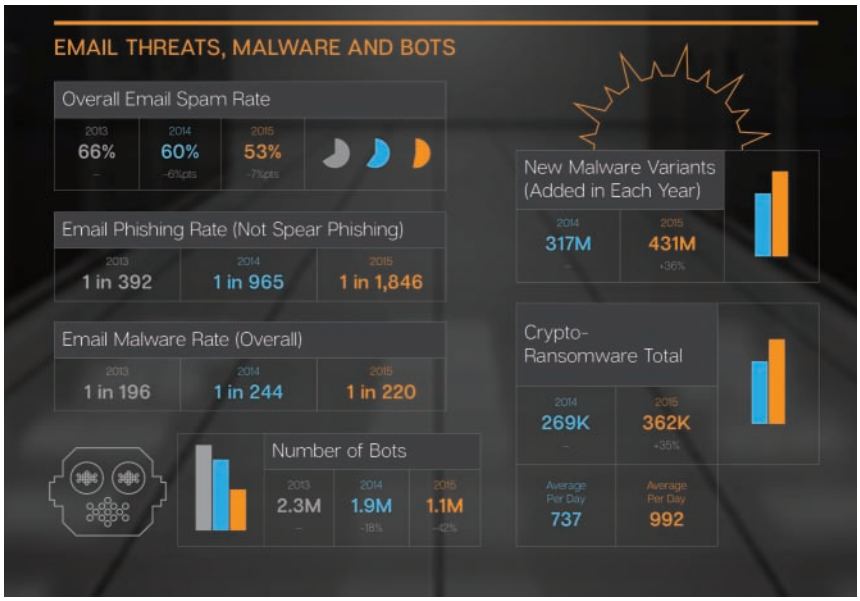
How SAM can help

SAM can provide you with a detailed report related to your software deployments.

Without an effective SAM program, some software can remain hidden from the view of IT leaders and operations team. This leads to a wider threat exposure because the regular system security operations, such as applying Patching or updates or security controls could potentially be missed on those hidden software.

According to the Internet Security Threat Report released by Symantec,[2] Ransomware continues to evolve. Last year, we saw Crypto-ransomware (encrypting files) push the less damaging locker-style ransomware (locking the computer screen) out of the picture. Crypto-style ransomware grew 35 percent each year. An extremely profitable type of attack, ransomware will continue to ensnare PC users and

One of the initial steps of a well-defined SAM program is to enable the IT function to get the first-hand information about the software implemented within the enterprise.



Source: Symantec

expand to any network-connected device that can be held hostage for a profit. These ransomwares are distributed to the targets through various means, and one of the channels is through software or applications downloaded by end users. Hence it is imperative to make sure the software or applications installed within the enterprise network are managed properly.

One of the initial steps of a well-defined SAM program is to enable the IT function to get the first-hand information about the software implemented within the enterprise. In addition to its inbound benefits of software compliance and operational effectiveness objectives, an effective SAM governance and risk management procedure should consider the step of software inventory as the starting point to assess the threat exposure associated with the unauthorized applications installed on the systems.

An effective SAM strategy will keep your systems secure, and will help eliminate the risk of purchasing software through unauthorized vendors. It will also make your existing software less vulnerable to external attacks.

It is important to actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and used, and that unauthorized and unmanaged software is detected and prevented from installation or execution.

Identifying expired, and unmatched software existing in your network well ahead of time will give you the ability to apply patches in a timely manner. For custom applications that require a specific over version of an operating system that is no longer supported by the manufacturer (E.g. Windows XP); knowing how many, and where this kind of software exists is a first step towards applying risk mitigation techniques.

The existence of Adware/unlicensed software/ cracks/ free software/ games/Trojans, and other shelf-ware, leaves your organization wide open to the threat of cyber-attacks, and for malware/ransomware to infect your infrastructure.

A good SAM strategy will help you identify these nuances in your environment and act on them in a timely manner. In most cases, users are unaware of these types of software breeding in their system; which is the nature and purpose of these agents. However, a well-defined software discovery (either via a tool or otherwise) as part of a SAM strategy can help reduce the threat of such exposure and save your organization millions of dollars and an embarassing moment. An effective SAM strategy will keep your systems secure, and will help eliminate the risk of purchasing software through unauthorized vendors. It will also make your existing software less vulnerable to external attacks.

SAM and security working hand-in-hand.

A well-defined and integrated SAM and IT security operations can help minimize the threat landscape by:

- Structuring a governance model to handle the asset management life-cycle;
- Supplementing the IT security function to manage cyber-threats associated with software;
- Integrating a SAM inventory collection

procedure to supplement the IT asset management program;
- Reconciling the inventory with an approved list of software and thus preventing unauthorized software before it is even installed within your infrastructure;
- Locating and weeding out renegade software; and
- Introducing mechanisms to identify redundant and outdated/obsolete software.

What next?

As it is evident that a software asset inventory and SAM can help organizations to effectively assess their inventory and understand the threat landscape, it is crucial to operationalize SAM through a systematic approach. Organizations should initiate a SAM program that integrates the people, process and technology domains together. This approach focuses on transformation, prioritizing opportunities for cost reduction and risk management.

To begin this journey, organizations should use a phased approach starting with:
- Performing a SAM diagnostics and benchmarking exercise; such as a software assets discovery and benchmarking SAM processes (to leading practices such as ISO19770-1) to understand the current environment; to the
- Formulation of a strategy and organizational structure. This includes building a corporate-wide SAM strategy based on the outcome of the SAM diagnostics and benchmarking exercise, and designing scalable SAM policies, processes, and procedures.
- Need determination and SAM Plan would be the next step. This includes establishing a baseline software inventory of your key software, and assessing the need for adequate tooling; to

Organizations should initiate a SAM program that integrates the people, process and technology domains together. This approach focuses on transformation, prioritizing opportunities for cost reduction and risk management.

- SAM Implementation into operations and continuous monitoring.

That makes SAM a seamless proposition.

Depending on the appetite and bandwidth of the organization, certain activities such as SAM diagnostics and baseline software inventory can be performed in parallel. Alternatively, the above activities can be outsourced to a managed service provider, ensuring cost benefits are maximized and operational efficiencies are realized.

SAM should be considered as a critical program along with other IT strategies and enterprise level initiatives and should be one of the critical strategic initiatives for any IT operations and risk management function.

by **Nithin Haridas**, Principal, Risk Advisory and **Huzaifa Hussain**, Senior Manager, Risk Advisory, Deloitte, Middle East

Endnotes

1. Gartner, Inc. | G00230816 -Software Vendor Auditing Trends: What to Watch for and How to Respond
2. www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf