USSELS • ATLANTA • HOUSTON • LONDON • BALTIMORE • CINCIN
ARIS • SALT LAKE CITY • ROME • PORTLAND • BRUSSELS • ATLAN
USTON • LONDON • BALTIMORE • CINCINNATI • PARIS • SALT
Y • ROME • PORTLAND • BRUSSELS • ATLANTA • HOUSTON • LON
ALTIMORE • CINCINNATI • PARIS • SALT LAKE CITY • ROME • P
ND • BRUSSELS • ATLANTA • HOUSTON • LONDON • BALTIMORE •
INATI • PARIS • SALT LAKE CITY • ROME • PORTLAND • BRUSSELS
NTA • HOUSTON • LONDON • BALTIMORE • CINCINNATI • PARIS •
KE CITY • ROME • PORTLAND • BRUSSELS • ATLANTA • HOUST
NDON • BALTIMORE • CINCINNATI • PARIS • SALT LAKE CITY • RO
RTLAND • BRUSSELS • ATLANTA • HOUSTON • LONDON • BALTIM
INCINNATI • PARIS • SALT LAKE CITY • ROME • PORTLAND • BRUS

SESSION PREVIEW WHITE PAPER

ITAM AND IT SECURITY
YOU CANNOT SECURE WHAT YOU DON'T KNOW
YOU HAVE!

IAITAM

www.iaitam.org

ITAM AND IT SECURITY REDUCE RISKS

Everyone knows how important the IT security team is to the organization, but few understand how closely the success of IT security depends on other groups within the organization. Information security is actually an organization-wide set of activities delivering information, support and cooperation. Imagine the difficulties an IT security team would encounter if they did not have:

- Organizational executives as stakeholders
- Human Resources for policy support
- Departmental management to promote education and compliance
- IT Asset Management (ITAM) for a “source of truth” on IT assets

It may seem surprising to see ITAM on the list, but ITAM delivers material value to IT security by building structure around the use of assets that documents the information about assets, influences decision processes, creates history and reduces asset chaos in the environment. Understanding the value of a strong relationship between ITAM and IT security is essential to protecting the organization. The IT department that fosters cooperation between ITAM and IT security benefits from more accurate information about the use of IT and ultimately improved goal achievement.

The importance of that cooperation is growing because IT trends are profoundly impacting IT security. Adoption of cloud-based applications and platforms and increased accessibility via mobile devices are some of the trends escalating the scope and requirements for IT security. Additionally, risks to the organization and its data are escalating as the digital invasion increases in sophistication, volume and malicious intent.

WHAT ITAM DELIVERS

IT security relies on a broad array of programs and tools to deliver risk management for the organization’s information, assets and systems. The obvious contribution that ITAM makes to security is in the management of contractual, financial and inventory aspects of the tools used by IT security. The story only begins at that point and the relationship continues through many aspects of risk management since the discovery and mitigation of risks depends on complete information about the hardware and software in the environment.

Risk mitigation includes the implementation of security standards and structures and the ongoing measurement and compliance to those standards. With a strong ITAM program, implementation and ongoing measurement are easier and more accurate. More of IT security’s time can be devoted to the monitoring and defense of the organization’s IT.

With risk management at the heart of IT security’s actions, any processes that provide clarity into the organization’s portfolio of assets and works to keep that portfolio as homogeneous as possible is going to be a help. IT asset management processes definitely fall into that category.

ITAM AND IT SECURITY REDUCE RISKS

SECURITY'S RISK MANAGEMENT

The processes that are part of risk management also provide insight into the support that ITAM offers. A major process within risk management is risk assessment. Risk assessment identifies, estimates and prioritizes risks from the operation of an information system. Information about IT assets and the lifecycle processes surrounding those assets are an important part of risk assessment. One project within risk assessment is the proactive vulnerability assessment. The work conducted during a vulnerability assessment is a good example of the complementary nature of ITAM to IT security. According to the National Institute of Standards and Technology (NIST), vulnerability is a "[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."

IT security executes a vulnerability assessment with the following general steps that clearly show the importance of asset information to a vulnerability assessment:

- Catalog assets and resources in a system
- Assign quantifiable value and importance to the resources
- Identify the security vulnerabilities or potential threats to each resource
- Mitigate or eliminate the most serious vulnerabilities for the most valuable resources

From identifying the assets within scope to the mitigation of the vulnerabilities discovered, IT asset management is responsible for providing accurate data about assets and for changing any lifecycle processes that are contributing to vulnerability.

The underlying theme for IT asset management is the importance of inventory processes throughout the lifecycle of the assets. Even in the asset retirement processes, ITAM is needed to build and maintain the inventory processes in order to reduce the chaos and unknowns in the environment.

THE GROWING SCOPE OF IT SECURITY

Securing assets is no longer a choice but a necessity. Laws dealing with privacy and standards like the PCI standard that describe what data needs to be secured are defining how the organization has to show that they are accountable and protecting the environment and the data.

Organizations have focused on IT security measures to block intruders from gaining access to their network and data. With that goal, organizations invested in perimeter firewalls, network security and limiting errant access via identity management. There is certainly more value to be derived from the existing investment in security processes and technology. Fundamentally, the security team needs to focus on reducing the risks to the organization by reducing the opportunity for some problems to occur and identifying the problems that do occur more quickly. IT asset management is part of the team that facilitates these efforts.

The bottom line for IT asset management is that the better the information is about the IT assets within the organization and in the cloud, the better security will be able to fine tune their detection processes. IT Asset Managers participating in cloud management have to take a leadership role in the contractual, financial and inventory management of cloud usage. Additionally, IT asset management needs to take an active role in governance information gathering and reporting across the IT resources in use, working with security to reduce risks to the organization.

FALL 2017
IAITAM ROAD SHOW

IAITAM, the IT Asset Management industry's global education provider is proud to announce a series of 1-day educational sessions at a location near you!

Join IAITAM's team of asset management experts and select industry peers addressing the issues pertinent to initiating, building and enhancing your organization's asset management program, the business side of IT.

SCHEDULE OF EVENTS

8:30a-9:00a Networking with Refreshments
9:00a-9:30a Opening
9:30a-1:30p One continuous session covering ITAM and IT Security, ITAM Program, ITAM and Cloud Computing, Software Audits, ITAM and ITSM and What Does an IT Asset Really Mean?
1:30p-2:30p Lunch
2:30p-3:30p Birds of a Feather, Closing

TICKETS FOR ALL FALL 2017 ROAD SHOWS ARE NOW AVAILABLE!

WWW.IAITAM.ORG

TOPICS

ITAM and IT Security
You Cannot Secure What You Don't Know You Have!

ITAM Program
What is the Most Effective ITAM Program for My Organization?

ITAM and Cloud Computing
Why do we need to Manage That?

Software Audits
Managing Audits as a Standard Business Practice

ITAM and ITSM
Understanding Best Practices and Standards in both Disciplines

What Does an IT Asset Really Mean?
Some of the latest buzz words: Big Data, the Internet-of-Things (IoT) and Shadow IT.