MPS Provider Best Practices: Security

The Managed Print Services Association

Our Mission

The mission of the MPSA and its members is to address and optimize businesses' office document management while enhancing the growth, efficiency, and profitability of the MPS segment through advocacy, marketing, education, research, standards, and a general community of interest. To reach these objectives, the MPSA provides community-driven best practices—like those contained in this document—to empower its members to make more informed decisions regarding their MPS strategies.

The MPSA defines Managed Print Services (MPS) as:

"Managed print services is the active management and optimization of business processes related to documents and information including input and output devices."

http://www.yourmpsa.org

DISCLAIMER: The MPS provider must determine the goals and objectives to be achieved and solved with the implementation of the best practices offered in this document.

MPSA
MANAGED PRINT
SERVICES ASSOCIATION

Contents

Introduction

Background

Security in the print environment is one of the most overlooked risk components of the network infrastructure, as it is usually deemed low risk by the Chief Security Officer, Chief Information Officer and Chief Technology Officer, in comparison to server and user terminal security. This mindset is beginning to change as customers become more educated about print security. They understand that security will create serious vulnerabilities for their organization if it is left unmanaged and there is no customer specific policy.

An MPS provider is seen as the trusted advisor to the organization for all elements relating to print and the infrastructure. It is therefore the responsibility of the provider to define the requirements to the client and project manage any potential client specific anomalies, including security related issues. This is true for both new as well as legacy devices in the fleet under management.

This whitepaper will in no way be a silver bullet for resolving the security requirements and risks of clients' fleets, however, the information included should provide MPS providers with an appropriate blueprint from which they can review and build on to ensure their clients are effectively secured against basic, as well as advanced, security threats.

Intent

Intent Statement

Through collaboration with the numerous subject matter experts in the MPSA Standards and Best Practices Committee, and those outside of the organization, the MPSA has compiled this set of focus areas and best practices. This document will offer MPS practitioners a set of best practices to consider when addressing security concerns in an end user's or customer's print environments. As part of a broader body of knowledge, this specific set of best practices will center on the overall security of the customer's network through their print devices. Additionally, this document will touch on the security of their printed documents.

This whitepaper is intended to aid an MPS provider's designation as a "trusted advisor" by focusing on an aspect of the print environment that is largely ignored and is becoming increasingly more vulnerable. These best practices should be included in any MPS program, but certainly not limited to MPS engagements.

Through thorough discussion with every customer, the MPS provider assesses which of these best practices are applicable to that environment and which may cause a general disruption to the day-to-day operation of the business. The success of an MPS program is not incumbent upon the application of these considerations today, however the growing concern around network security could certainly mandate this to be a vital component of an overall offering in the near future. As with all information, the MPS provider should determine the goals and objectives to be achieved and solved with the implementation of these best practices.

Focus and Scope

Security best practice as part of an MPS program should align with the overall information security strategy of the customer. MPS providers must understand that security goes beyond the device, as printers have continued to evolve and now are like any other Internet Of Things (IOT) endpoint. Security plays a role throughout the services lifecycle. It starts with the initial definition and analysis of business requirements in Service Strategy and Service Design, through migration into the live environment within Service Transition, through to live operation and improvement in Service Operation and Continual Service Improvement.

The focus and scope of this whitepaper includes best practices for security services in MPS engagements and focuses on the impact of the fleet, documents and users. To deliver an effective MPS offering, providers need to ensure that they have an industry-standard measurement. We propose benchmarking any offering against Information Technology Infrastructure Library (ITIL) or Specific, Measurable, Aligned/ Achievable, Relevant, Time Bound (SMART) standards to provide the best service in the most affordable and efficient manner.

With any security program, there are specific worldwide, regional and country specific regulations that provide governance. We have listed some of these regulations and certifications below, and this is by no means an exhaustive position but rather a view of those which are most predominant in the MPS industry. It is key that an MPS practice research each of these in-depth to gain insight on what is applicable to the specific customer industry vertical they are engaging, as these elements differ considerably from one industry to the next.

These regulations and certifications are constantly updated which requires constant review of your MPS security program and its relevance to the latest refreshed standards.

Industry-specific regulations

- Section 508 of the Rehabilitation Act of 1973
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Gramm-Leach-Bliley Act (GLBA)

Top Hardware / Firmware / Network Certifications:

- Federal Information Processing Standards (FIPS)
- NIST references FIPS certifications for their standards
- Common Criteria (NIAP/CCEVS Certification, ISO 15408)
- IEEE 2600

This whitepaper has been separated into two sections which will allow the material to be focused in the major areas we believe are critical to MPS security. These sections are Hardware and Software, which will have their own subsections to better define the content.

The table below displays the MPS components within the ITIL framework, with additional columns for 12 high-level security service areas included in this best practice document. This is a high-level table of all the components that could be included in an MPS security strategy. This whitepaper is focused on the more important elements which allow for a provider to achieve “quick wins” within their client install bases.

MPS SERVICE FRAMEWORK: MPS COMPONENTS AND HOW THEY FALL WITHIN ITIL FRAMEWORK

	SERVICE STRATEGY	SERVICE DESIGN	SERVICE TRANSITION	SERVICE OPERATIONS	CONTINUAL SERVICE IMPROVEMENT
MPS COMPONENTS	• Assessments • Document Policy • Business Requests • Business Case • Perfect Measurements • Financial Considerations • Sourcing Decisions	• Geography • Onsite Inventory • Management • Device Monitoring/ Management • User Management • Technical Skills • MFG Support • Warranty • Equipment • Contract Management • SLA Development • Sustainability • Security • Multi-vendor Support	• Device Installation • Device Configuration • Fleet Labeling • Human Change Management • Implementation Plan • Communication Plan • Testing & Validation • Knowledge Base/FAQs	• Ticketing • Help Desk/Support • Exception Requests • Supply Fulfillment • Break/Fix • Monitor/Manage Devices • Policy Governance • Account Delivery • Management	• Reporting • Billing • Optimize Fleet • Optimize Behavior • Process Improvement • Workflow Improvement
SECURITY ALIGNMENT	• Security and Compliance Assessment	• Fleet Design / Policy Design • Rights Management / Secure Remote Management / Software • Secure Pull Printing • Secure Workflow • Network Security Skills / Certifications	• Data Storage / Security and Hard Disk Configuration • Secure Device Disposal • User Training / (Change Management)	• Security and Firmware Governance • Secure Document Disposal Services / Data Leaks Protection	• Security Reporting and Review

DISCLAIMER: The MPS provider must determine the goals and objectives to be achieved and solved with the implementation of these best practices.