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
SECRUITY 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

Hardware and Networking Section

Fleet Design / Policy Design

Definition

The fleet and policy design is defined as the plan used to minimize data breaches and unauthenticated user vulnerabilities. The definition includes the fleet hardware e.g. MFD hard drives, the software which may be used to process documents and manage the hardware, as well as the user who may want to access the print services. Fleet and policy design typically comes after a risk assessment and should reveal any security vulnerabilities.

A fleet design is a flexible plan of hardware and/or software integration into a customer's environment which mitigates existing security risks and does not introduce new vulnerabilities. For example, using an MFD device at a financial institution which does not support secure communication protocols like SNMPv3, could be a major failure point for maintaining a secure environment as the financial vertical invariably prescribes SNMPv3 as a standard. It is flexible because its implementation may be subject to phases and budget constraints.

Policy design is a plan of ongoing control over the unauthenticated access to print services and the devices used to deliver those services. For example, requiring authentication cards and the card readers to be used to print documents, is a policy design. A policy design example may be to designate or approve for procurement a specific vendor, make or model due to its security features.

Considerations

Design Input

Every design needs a starting point and actual usage data is important for fleet design. Data about the current state, which may include fleet inventory and volume, user access limits, security vulnerabilities, etc., drives the design. A good source for this data is the compliance or risk assessment report. This report is the product of a thorough assessment of the customer's current hardware, software, network and high-level user environment. It should be conducted by any MPS practitioner who wants to ensure they have the most accurate and relevant environment data in hand to use for design.

The risk assessment report reveals vulnerabilities (what needs protecting) from both inside the customer environment and outside the firewall. Common design concerns are:

- Customer data - sensitivity to risk. For a high-security environment, both document and device data may require some authentication and encryption technology. For example, documents cannot be left on the output tray and may require user authentication to process the job. Another sensitivity is where the data is stored, for example, data may not be permitted to be stored outside the firewall at a Hosted 'Cloud' facility. Print management tools that use the Cloud to manage devices may not be permitted, perhaps only on-premise tools that store data locally are allowed. Finally, a consideration to the location area where the device is accessed.

- Accessibility to print services – security versus productivity. For example, the customer may require only certain individuals be granted access to specific services like print, copy, scan or content access. Services and the services that grant access to Single Sign-on (SSO) require some user authentication, typically based on checking of a user

against an Access Control List (ACL) system. Typically, single- or two-factor authentication is used via a universal card, which may also grant access to a physical location, e.g. a building, and allow a service like pull-printing.

- A responsible party for security authority needs to be identified and brought into the fleet design process. This may be the IT security (sec) department or an outside party. Ultimately, they will have input and approve the fleet design and participate in its ongoing use.

Considering what the customer views as important to security allows the MPS provider to propose a fleet design, and the resources and costs required, to meet the accepted proposal.

Fleet and Policy Design

Things to consider in the design are typically the practical elements like printers/documents and how they interact with users. These elements or factors may be:

- Printer and user physical location – how far from the print service is acceptable, e.g. device mapping
- Make and model of the devices used in the design – use existing fleet or replace and add fleet
- Security capabilities of the printer – do they support authentication technologies
- Device components like MFD hard drives – is the data vulnerable to attack
- Devices accessible over the internet via IPPS – known cases of Denial of Service attacks due to internet access
- Data storage – is the data stored in the Cloud or locally (inside the firewall) stored and managed
- Software management tools – are these apps secure enough, self-certifying or use certifying authority (CA)
- Infrastructure use – are there existing security apps to leverage, e.g. SIEM[1] applications
- Server components, print servers and document servers – are they vulnerable to attack
- User access to services – how restrictive should access be and what security mechanisms should enable it
- Security authority and review – what parties manage the ACLs and sign off on the design
- Security technologies deployed – do the encryption and authentication solutions meet the target security level

Another factor affecting design is the level of automation desired by the customer. Typically, the designs they require are more of a manual implementation which causes higher overall program costs more than automating operations and oversight. For example, there are various forms of authentication including manual inspection of ID cards or using automation where a software application can verify a user through a PIN code and card scan. The cost constraints of the customer may dictate design considerations.

Ongoing Design

Security threats change as do MPS requirements. Consider periodic fleet and policy design reviews. These reviews can be coordinated with periodic security risk assessments.

[1] SIEM Security Information Event Management

Benefits

Professional Service Revenue

By offering fleet and policy design services, the dealer opens the door to providing a critical service which can be highly profitable. This can be a new source of revenue that leverages the expertise the dealer has in the print industry by combining a highly sought-after IT skill in security. Security experts are among the most highly paid IT professionals but often lack the knowledge and experience in print. This presents an opportunity for dealers to add a risk assessment and follow-on security service to their professional service revenue.

Customer Loyalty

Dealers can build customer loyalty by being a mission-critical supplier. Security is a mission-critical process for most organizations and, to the degree the dealers involve their services with the security, they can become indispensable to their customers.

Fleet Design / Policy Design for Remote Working

Consider how the design of your fleet should address pandemic related concerns. Select devices with extended service intervals and extra high yield consumables to avoid touch points. Adopt placement methodology that locates MFD's away from seated users to avoid potential infection of users that are seated nearby devices. Determine how workflow solutions can help minimize infection at the device touch points.

Network Security Skills / Certifications

Definition

To be considered a trusted advisor in assisting your clients with security best practice policy implementation, it is key to ensure you can portray credibility. This can only be achieved by underpinning your offering with the required skilled and certified individuals who will be responsible for the intellectual property within your organization. This team will provide educated consultancy and guidance for the implementation of a security policy and the client will feel comfortable in allowing these individuals to work on and configure their environment.

Considerations

The first thing to consider is at what level do you want to build your Managed Service offering. Are you going to restrict yourself to the print environment or are you looking to move into Managed IT as a program for your organization? This market engagement desire will dictate the level of engineer skill, experience and certification you will need to attract and employ.

The following table provides a high-level view to consider for the level of offering you wish to provide:

	MPS	DMS	MIT (End Point)	MIT (Server)
Experience (5 Years Minimum)	✓	✓	✓	✓
Experience (10 Years Plus)	✗	✗	✗	✓
Hard Skills				
IDS/IPS, penetration and vulnerability testing	✓	✓	✓	✓
Firewall and intrusion detection/prevention protocols	!	✓	✓	✓
Secure coding practices, ethical hacking and threat modeling	!	✓	✓	✓
Windows, UNIX and Linux operating systems	✓	✓	✓	✓
Virtualization technologies	!	✓	✓	✓
MySQL/MSSQL database platforms	!	✓	!	✓
Identity and access management principles	✓	✓	✓	✓
Application security and encryption technologies	!	✓	✓	✓
Secure network architectures	✓	✓	✓	✓
Subnetting, DNS, encryption technologies and standards, VPNs, VLANs, VoIP and other network routing methods	✓	✓	✓	✓
Network and web related protocols (e.g., TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols, etc.)	✓	✓	✓	✓
Advanced Persistent Threats (APT), phishing and social engineering, network access controllers (NAC), gateway anti-malware and enhanced authentication	!	!	✓	✓
Soft Skills				
Strong Communication Skills	!	✓	✓	✓
Prepared to work long hours	✗	!	✓	✓
Handle stress well	✗	!	✓	✓
Extended Certifications to Consider				
CEH: Certified Ethical Hacker	!	!	✓	✓
CCNP Security: Cisco Certified Network Professional Security	!	!	✓	✓
GSEC / GCIH / GCIA: GIAC Security Certifications	!	!	✓	✓
CISSP: Certified Information Systems Security Professional	!	!	✓	✓

Must Have	✓
Beneficial if Available	!
Nice To Have	✗

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

Benefits

This of course is not an exhaustive list or a silver bullet, however, it provides an indication of what you should expect from a team that you would feel confident to be able to architect and support your clients. This will mitigate contractual breach ramifications by not providing an appropriate well-structured and industry best practice aligned security policy.

Over and above protecting your business, you will position yourself strongly to be considered for additional professional services opportunities by the client. You will also be in a position to promote continuous review of their environment to maintain relevance and alignment with latest industry threats and technologies.

Data Storage / Security and Hard Disk Configuration

Definition

It is of upmost importance that the information passed on to devices throughout the network is sent in an encrypted state as well as processed and stored on the hard drive (HDD) memory of those devices in the same encrypted state. This will ensure there is no potential for data leak and that PCI and HIPAA compliance, for example, is maintained.

An appropriate security policy also assists in removing some of the responsibility from the end user to ensure the data is protected through hard coding and automating the process for them and the organization.

Considerations

When engaging a customer environment, it is key to do an initial assessment to understand the complexity of their fleet. This would be defined by the deployed models, their age and their encryption and overwriting capabilities within their ecosystem. These elements dictate the level of security available to configure on the HDDs as well as whether HDDs are even installed at all.

Bearing the above in mind, you need to ensure that the HDD and the communication to the devices are managed through a policy which would include the following and more:

- Encrypted HDDs (if applicable)
- HDD image overwrite / sanitization
- HDD physically secured inside device chassis
- HDD retention for customer if swap out required

Benefits

While encryption addresses data at rest on the disk, further security can be achieved by enabling capabilities which overwrite individual job data either on-demand or the entire area of the disk where job data is processed. These features add an additional layer of security and can be deployed as customer requirements dictate. If the HDD is secured physically through technological requirements of the above best practice elements, it will ensure that the customer is well protected from external or internal malicious intent. It is important to think in the same way a hacker would in viewing the environment in an attempt to gain access and steal critical and confidential information.

This leads to the next point: information may be secure within the client environment, however in many cases, what happens to the device and its HDD after it leaves is not taken into consideration.

Data Storage / Security and Hard Disk Configuration for Remote Working

Work from home, in many cases, exacerbates the problem of managing confidential information stored on the hard drive of printers. Every print job produced by a printer has to route via the hard drive in order to be rendered and printed. Therefore, that document image resides on the hard drive until it is overwritten due to capacity being full or forcibly scrubbed by appropriate settings as defined above. Your print ecosystem has most likely doubled or tripled due to users working from home, therefore so has your risk. The other issue faced is when home office printers are replaced or disposed of by the end user at home, they invariably end up in land fill and not scrubbed and destroyed in the same way IT would / should treat a printer or laptop hard drive. Therefore, the question to be asked is: if this device were on your corporate LAN, how would you treat it and does something need to change?

Firmware/ BIOS - Threat Detection

Definition

Printer BIOS (basic input/output system) is the program a personal computer or printer microprocessor uses to get the operating system started after you turn it on. It also manages data flow between the printer's operating system and computer.

Firmware is a software program or set of instructions programmed on a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.

Considerations

BIOS firmware is a key target for cyber attackers, especially through malware. Once they have installed malware, hackers can then use the printer to control or gain access remotely. To adequately protect these areas from vulnerability and control of the printer, there needs to be a layered security approach. Areas of practices for security around printers include:

- Anti-virus/Intrusion Protection - hardware or software solutions to validate firmware for any anomalies and alert or stop the intrusion.
- Bios Protections - hardware or software capability to validate the integrity of the BIOS during startup and operation.
- Updates/Patch management - process to receive and push out these updates and patches as they become available.
- Setup/Configuration Standard and Policy - help control things like resetting factory default password for settings access.
- Firmware Whitelisting – software which monitors the device's system files and ensures that no modifications have been made.

Benefits

Protecting the BIOS and firmware on a printer is an important part of preventing unauthorized access to data, documents, or network access through the printer. Putting processes, such as the ones above, will provide another layer of security around your network and information.

Firmware/BIOS for Remote Working

Work from home use of personal printers creates challenges in that you often don't have an IT team managing your device(s) and ensuring security policies and patch updates are routinely setup, checked, and managed. It is crucial to address these items to protect your device(s), and subsequent network and data from attacks. As employees, we are obligated to ensure these steps are taken on our personal devices. Following the above steps in the considerations area will ensure the proper protections exist for the printer Firmware/BIOS.

USB Port Security

Definition

A USB flash drive is a device used for data storage that includes a flash memory and an integrated Universal Serial Bus (USB) interface. Most USB flash drives are removable and rewritable. Physically, they are small, durable and reliable. The larger their storage space, the faster they tend to operate. USB flash drives are mechanically very robust because there are no moving parts. They derive the power to operate from the device to which they are connected via the USB port.

In terms of printers and MFD's, a USB drive is often used when a customer has a need to print a document or scan a document without the use of a PC.

Considerations

Utilizing a USB port on an output device can provide some additional convenience in terms of workflow for the user community without adding complex technical solutions or overhead.

- Disable USB ports on all output devices if not required by customer workflow or service-related activities. Limit use of a USB port to printing documents and limit use of scanning unless required (minimize data theft).
- Choose an OEM partner with malware detection that includes USB port monitoring.
- Ensure the authentication model includes the requirement to log in to access the print from /scan to USB functions.
- Enable logging of a USB port to record access and actions associated with USB port use.
- Consider if any hardware accessories will utilize one or more of the available USB ports.
    - A device may only have one port available and connecting a peripheral may mean there are no ports available for users
    - Ensure your security model and device configuration considers the fact a user could unplug a connected peripheral and hijack the port for nefarious purposes

Benefits

Factoring USB ports on output device security models is an important component of a comprehensive security program. Benefits include reducing the potential for data theft through imaging, unauthorized use, costs associated with printing and the potential for the introduction of malicious software into the environment.

Portable and mobile storage devices are significant players in most corporate offices. Ensuring proper protection with a best practices policy and strict enforcement offers significant risk reduction—and can prevent long nights on data breach investigations.

USB Port Security for Remote Working

In a work from home scenario, the USB port on your endpoint devices are critical access points to your organization's network. While these access points on your laptops and output devices provide for a convenient way to transfer, upload, and share files, these access points are also vulnerable to security threats, threats that can ultimately bring an organization to a grinding halt. It is important that your organization has a strong policy around USB port management. These policies can either lock down the ports through modern device management capabilities or at minimum provide guidance and governance on how the ports are utilized through ongoing training.

Password Management

Definition

Passwords are still used to access most devices and applications used in business and personal life today. It is a secret word or phrase that must be used to gain admission to something. Because there are different rules or combinations on letters, numbers, symbols, capitalization, etc. for these devices or systems, it has proven challenging for people to manage these in a secure manner. Effective password management is an important function for security and efficiency reasons.

Considerations

Passwords are fundamental for information security. They are used as a first-line defense in securing almost all electronic information, networks, servers, devices, accounts, databases, files, and more. Most of us now have a multitude of passwords we need to somehow track and remember.

From a security perspective, these passwords must be protected. Passwords can be compromised in many ways:

- User devices may be compromised with a keylogger or similar malware and disclose user input to an attacker.
- Users may write them down or share them, compromising secrecy.
- Passwords can be guessed, either by a person or a program designed to try many possibilities in rapid succession.
- Passwords may be stored or transmitted over a network either in plaintext or encoded in a way which can be readily converted back to plaintext.

Each of these vulnerabilities create an opportunity for an attacker to acquire password values and consequently impersonate users.

Password compromise is still the leading cause behind most data breaches and it important to follow secure password management practices. Secure password management requires unique passwords to be used for each account. Passwords must be both long and complex; comprised of numerals, mixed-case letters, and special characters. They also should not be words or names of anything which could be associated with their owner. Finally, passwords must be changed frequently. Password management applications are recommended by most IT security experts. Some examples of the most popular ones are Last Pass, Dashlane, and Keepass.

In addition to password management applications, there are also manual methods that can be used to track passwords. These include storing electronically in an encrypted file, storing in browser built-in password managers, or even trying to just commit to memory. Regardless the method, managing passwords must be a priority for securing unwanted access to information and rights.

Benefits

By establishing processes for creating, storing, and managing passwords, data and systems will be far less vulnerable to unauthorized access. It is also an important step for means of improving efficiency in access and use of data and systems.

USB Port Security for Remote Working

Password management dynamics are even more challenging when facing a work from home scenario. Depending upon your organization's authentication methods, your remote system access may require multiple levels of authentication steps. These steps may introduce opportunities for typos and account lockouts. Self-service password management processes must be evaluated to ensure you can properly support your end users and ensure productivity is not impacted. End users also need to do their part. While it may seem enticing to post those passwords on a sticky note in your home office, there is a chance that data could be seen through video conferences.

Protocols

Definition

There are multiple protocols that need to be considered in the design of a secure MPS environment. The list of protocols is as follows and each needs to be taken into consideration regarding the requirements of each client's IT infrastructure environment. There may be software and systems reliant on certain protocols being available and the requirements need to be weighed against the potential risk. Any protocols not used regularly should be disabled to minimize vulnerabilities.

- **SNMP / SNMPv3** - Simple Network Management Protocol (SNMP) is a set of protocols for network management and monitoring that improves security and privacy. These protocols are supported on printers, and other network components and devices.
- **Telnet** - A protocol that allows a connection to remote computers (called hosts) over a TCP/IP network (such as the Internet). Using **telnet** client software on a computer or printer enables a connection to a **telnet** server (i.e., the remote host).
- **Bonjour** - Apple's version of the Zero Configuration Networking (Zeroconf) standard, a set of protocols that allow certain communication between network-connected devices, applications and services. Bonjour is often used in home networks to allow Windows and Apple devices to share printers.
- **FTP** - File Transfer Protocol (**FTP**) is a standard network protocol used for the transfer of computer/printer files between a client and server on a computer network.
- **IPP -** (**I**nternet **P**rinting **P**rotocol) A protocol for printing and managing print jobs over the Internet using HTTP. The protocol includes authentication and encryption.
- **NTP -** Network Time Protocol (**NTP**) is a TCP/IP protocol used to synchronize computer clock times in a network. The term **NTP** applies to both the protocol and the client-server programs that run on computers/printers.
- **LPR / LPD -** A platform-independent **printing protocol** that runs over TCP/IP. Originally implemented for BSD Unix, its use has spread into the desktop world and is a de facto industry standard.
- **SMB** - Server Message Block Protocol (SMB protocol) is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network.

Considerations

Many printers have insecure and unnecessary protocols enabled by default (e.g., Telnet, HTTP, FTP). Leaving these services enabled provides attackers the ability to access printer data directly. While a practical joker with limited knowledge of printer job language (PJL) might only Telnet to change the "Ready" message to something cute ("Insert Coin"), a more malicious attacker could potentially browse the printer's hard drive and view all the data stored there.

Disabling these services prohibits your printer from being used for unintended purposes, such as hosting pornography, or as an FTP server for copyright protected music and movies.

Benefits

Having all the protocols configured appropriately to the customer's environment and ensuring unnecessary protocols are deactivated ensures a more secure ecosystem. This will minimize the target surface for hackers to potentially compromise the device and results in a more secure solution.

Protocols for Remote Working

With devices now being off the corporate network and security firewalls, it's even more important to ensure that the print devices are appropriately configured. If unnecessary protocols are left open or unmanaged, hackers have the ability to gain access to devices as many new home office printers are now Wi-Fi capable, are therefore on the network and can act as an entry point to other devices on the same network. Now take it one step further, where many organizations still run on premises applications, such as their ERP system which requires the end user to open a VPN tunnel to connect. The hacker now has a gateway to the corporate network. If anything, it may be even more important to ensure home office printers are correctly configured and maintained, as they are not readily accessible or visible by IT and therefore easily forgotten about until an issue is experienced.

Authorization (Certificates / HTTPS)

Certificate Management

Definition

Certificate authority (CA) certificates are needed to allow a device to trust and validate the credentials of another system on the network. Without a CA certificate, the device has no other means to determine whether to trust the certificate that is presented by the system to create a secure connection.

Considerations

Most devices use certificates for HTTPS, SSL/TLS, IPsec and 802.1X authentications. Because they can be easily integrated with PKI environments, these devices can set up trusted communication transportation for 802.1X and IPsec certificate authorization for validating domain controller certificates and Lightweight Directory Access Protocol (LDAP), Secure Sockets Layer (SSL) or any other service that uses SSL or Transport Layer Security (TLS). The device has a self-generated default device certificate by which the device can be uniquely identified. For some operations (for example, 802.1X and IPsec), the default device certificate needs to be upgraded to a certificate that has been signed by a CA so that other devices trust that specific device. A process is defined for upgrading the self-generated device certificate to one that has been signed by a known CA. For devices that are part of an Active Directory environment, this process has recently been simplified with an application installed on newer devices.

The Certificate Management menu is used for configuring printers to use device certificates for establishing SSL, IPsec and 802.1X connections. Additionally, devices use certificates for LDAP over SSL authentication and address book lookups. The configuring process for devices consists of the following steps: 1) Load the CA certificate for a certificate authority in the device. 2) Create a device certificate or use the device default certificate. 3) Create a CA-signed certificate with that device's certificate data using a certificate request file submitted to the CA. 4) Load the CA-signed certificate in the device.

NOTE: This process can be greatly simplified with a new Automatic Certificate Enrollment application, which is available when an Active Directory environment is used. Different manufacturers' firmware generates 2048-bit RSA private keys and uses them to self-sign an X.509v1 device certificate. Current firmware uses SHA-256 hashing for signatures, while some older firmware might use weaker hash algorithms. The device private key is never externally accessible.

Platform A devices within Active Directory environments also support the ability to look for updated certificates at periodic intervals.

Benefits

Certificates are the trust mechanism underlying much of public key infrastructure (PKI). A device's certificate management features support this trust from two viewpoints:

- Certificates enable devices to trust network services, guaranteeing the identity of the servers being accessed.
- Device certificates enable devices to be trusted by other network services if a trusted CA has signed the device certificate.

Certificate Management for Remote Working

In remote environments, certificates will become the responsibility of the employee. Unless the company provides the employee a VPN router or network, IT will not be able to manage certificates. A better route would be to use Cloud Printing, as in that case, IT can manage the security of the document and the printer is only used to print an encrypted document that is safe from hacking, virus's or spam. Most VPN's will not allow a user to be on a local network and a VPN at the same time.

HTTPS

Definition

Networked printers and MFPs can be securely managed with HTTPS from each device's Embedded Web Server. For more security, HTTPS can be used to manage the device remotely conveniently and effectively.

The most common means to remotely configure networked devices is through the device's Web interface. Device settings can be configured by pointing a browser to its IP address or host name and providing the proper credentials. However, browsers and the HTTP traffic associated with them, are not inherently secure. An intruder can detect the network traffic used in the Web session and determine the device's password.

Considerations

Most manufacturers' devices include an Embedded Web Server. When a browser is pointed to a device's address with the "https://" prefix, the device and the client system negotiate an SSL connection. This involves the device passing its x.509 certificate to the client system to establish its identity. Because the device's certificate is self-signed by default, the client typically presents a warning to the user (whether and how this happens depends on the settings of the Web browser). The client system can choose to trust the self-signed certificate, and thereafter does not receive further warnings. Alternatively, the device's certificate can be signed by a CA. This can be an external CA or a CA that is internal to the customer's environment. The device's Web interface includes a certificate management page that facilitates this process. Replacing the self-signed certificate with a CA-signed certificate avoids the warnings associated with the HTTPS session. The HTTPS session is built on an SSL connection in which all exchanged data is encrypted. This protects the contents of the session against eavesdropping and enables secure remote management of the device.

Benefits

The benefits of using HTTPS for web sessions include:

- Ease of use in establishing a connection for the end user. Point the browser to "https://" instead of "http://" and the device and browser will automatically process the rest.
- The encryption of all data exchanged through the browser, including passwords and any other settings that are set or viewed.
- Supported by most commonly used Web browsers. HTTPS and SSL are widely used standards.
- Integration in pre-existing CA or PKI environments. The device's certificate that allows the SSL session to be established can be signed by a CA.
- Web sessions can be conveniently and effectively secured.

Device Authentication (RFID Access / Walk Up Functions)

Definition

When a function such as Scan to E-mail is selected, the MFP can require the user to authenticate before proceeding. This limits device access to valid users only and enables the MFP to identify who is performing the function. It is suggested that not only user authentication is supported, but authorization as well. This allows device administrators to grant individual users and appropriate groups the right to access a particular device function or functions, while restricting other users or groups from using the same functions.

With this capability, individual users or group members can use their network username and password to access the device. The device can determine whether the user has access to the appropriate functions, based on the access rights configured by the device administrator. This level of control applies to network access through the device's web server, as well as to the configuration and use of the device through the touch-screen interface. The device can also be configured to authenticate and authorize users against internal accounts, passwords and PINs—as well as against a corporate directory through an encrypted channel. These authentication methods are secure over an SSL channel and are compatible with Active Directory and other directory-server platforms. An important aspect of user authentication and authorization is that users can enter their normal, or corporate, user ID and password. Users should not, and do not, need to remember a special set of information to use a device. Instead, the device makes use of the corporate directory to validate the user's credentials against the standard, centralized database.

Considerations

When network authentication is used, a user authenticates their identity by using their normal user name and password, just as they do when logging in to their workstation or laptop. This keeps the process simple and intuitive. Faxes sent with networked fax servers can automatically send an e-mail confirmation of the fax to the sender's e-mail, because the MFP recognizes who is sending the fax. The process of authenticating users is flexible. Devices can use a variety of internal authentication mechanisms and network directory authentication mechanisms and protocols to validate user credentials. Devices can be set up to use device internal accounts, device passwords, device PINs, Lightweight Directory Access Protocol (LDAP) [with or without SSL/TLS], Kerberos, LDAP+GSSAPI and NTLM for authenticating users. Support for a wide array of authentication protocols means that the device user authentication function is compatible with an array of network environments, including Microsoft Active Directory, Novell eDirectory and other directory environments that support LDAP. Secure user authentication protocols, such as LDAP with SSL/TLS configured, Kerberos, LDAP+GSSAPI and NTLM, protect users' credentials during the authentication process.

The device manages authentication and authorization with one, or more, of the following methods:

- PIN or Panel PIN Protect
- Password or Web Page Password Protect
- Internal accounts
- LDAP
- LDAP+GSSAPI
- Kerberos 5 (used only in conjunction with LDAP+GSSAPI)
- Active Directory
- Card access
- NFC/Cell-phone app access

To provide low-level security, limiting access to a printer – or to specific functions of the printer – can be achieved by requiring entry of a PIN or password. Alternatively, Panel PIN Protect and Web Page Password Protect, for some printer models, will limit access to those who know the correct code. This type of security might be appropriate if a printer is in the lobby or other public areas of a business so that only employees who know the password or PIN are able to use the printer. Because anyone who enters the correct password or PIN receives the same privileges and users cannot be individually identified, passwords and PINs are considered less secure than other building blocks that require you to be identified, or both identified and authorized.

LDAP and Active Directory can be utilized to manage additional security measures beyond walk up functionality and it is suggested that a more in-depth review be done on these elements by a certified resource. This will enable the ability for competent troubleshooting with customer IT regarding any issues which may arise concerning the print environment and these elements.

Access Controls

With multiple access controls, you can choose from a list of available security templates to control local and remote access to specific menus and functions and workflows. You can even disable functions entirely. Examples of walk-up functions that can be controlled are:

- Copy
- Scan to email
- Scan to fax
- Scan to FTP
- Print held jobs (such as confidential print jobs)
- The ability to print jobs from a portable USB memory device (for example, a flash drive)
- The ability to scan jobs to a portable USB memory device
- USB device access
- Launching embedded applications

Access to installed applications on the Device

Local and remote access to several different administrative menus can also be managed with access controls. Examples of menus that can be controlled are:

- Security menu
- Settings menu
- Network/Ports menu
- Configuration menu

Device management functions can also be restricted with access controls. Examples of device capabilities that can be controlled are:

- Firmware updates
- Control panel lock
- Web importing and exporting of settings
- Remote management

Access to these functions can be set by selection of a permission for that function.

Benefits

The benefits of user authentication and authorization include:

- Securing an MFP by limiting who can use its control panel to access functions such as Copy, Color Copy or Scan to Network.
- Avoiding anonymous e-mail by inserting the identity of the authenticated user in e-mail generated by the Scan to E-mail function. With additional configuration, the Scan to E-mail function can also limit e-mails to a predetermined destination (for example, only send emails to the logged in user or a user account listed in the address book should the device authentication software not allow this level of control) so that the e-mail cannot be sent to arbitrary destinations.

Control Panel Lock

Definition

With the control panel lock feature, a device can be placed into a locked state so that the control panel cannot be used for any user operations or configuration. It cannot copy or scan jobs. It cannot be reconfigured with the control panel, and incoming jobs do not sit exposed in the output bin. If the device has a hard disk, incoming print and fax jobs are stored on the hard disk instead of printed. The device can be unlocked by entering authorized user credentials, at which time, the held jobs are printed and the device resumes its normal operation.

Considerations

The control panel lock is configured by creating an authentication building block and applying it against the control panel's lock function access control through the device's Embedded Web Server. Depending on the type of authentication building block and the security template that is applied to this function access control, the user can enter a device PIN, a device password or network credentials to lock or unlock the device at its control panel. This feature requires the installation of a hard disk. When a device is locked, the control panel does not allow any interaction other than specifying the appropriate credentials to unlock it. While locked, incoming print jobs and faxes are not printed, but stored in the device's hard disk. If hard disk encryption is enabled, then jobs stored in the hard disk are encrypted. When the device is unlocked, jobs received during the locked period are printed. Any confidential print jobs received during the locked period are not printed, but they are available through the typical "confidential print job" interface on the device's control panel.

Benefits

The features and benefits of the device lock feature include:

- Devices can be secured with a simple method so that during off hours, scanning and printing operations are not permitted.
- Jobs printed to a locked device cannot be stolen from the output bin.

Networking

Definition

A thoughtful approach to networking is an important component of any MPS program and overall security model. Best practices include reviewing wired vs wireless connectivity as well as the use of static IP's and DNS reservation.

Considerations

Wired - Although wireless connectivity may be convenient, a best practice is to hardwire output devices to the network. Utilizing a wired connection offers a higher level of security by reducing the potential for infiltration from threats not physically connected to the same network as the printer. An additional benefit to service providers is minimizing the tendency of device relocation without following proper change controls.

Wireless - In an environment where wireless is utilized, appropriate precautions should be employed to minimize risk. At minimum, the following best practices should be observed in a wireless network.

- Select a wireless security option of WEP, WPA, or WPA2 (we suggest WPA or WPA2)
- Ensure the wireless network is secured with a non-default password
- Change the default password on the printer to a secure cypher
- Disable remote administration of the output device
- Disable any not needed ports and protocols

Whitelisting - The practice of using DNS or reservation occurs when a specific device MAC address is associated with a specific IP number, and often, a specific port number. Commonly referred to as whitelisting, this practice ensures that only authorized devices through authorized connections are accessing the network. By whitelisting an output device, you functionally eliminate the possibility of a threat hi-jacking the wall port and the IP of an output device to access the backbone.

Benefits

The benefits to reviewing the networking component of your print policy are:

- Reduced risk of a compromised device from an attack outside of the building or wireless range
- Eliminate potential for the output devices connection to be utilized by unauthorized people or devices
- Containing costs associated with additional network hardware (IE: access points)
- Reduced unauthorized device movement within a site

Certificate Management for Remote Working

Any device that is placed on a network must be evaluated with respect to security. How does the device protect itself from unauthorized access? Does the device expose the network to any form of vulnerability? What sort of information does the device process, and what are the security considerations related to that data? These and many other questions are appropriate to ask concerning any networked device, including networked printers. In the case of printers on a local network that 99% of remote employees will be on, the company would be better to secure the documents that are

being printed from any company provided computer, ERP or CRM. If the IT dept is tasked with managing all of the local networks that employees use, their workload is increased. In most cases, employees can have different Internet connectivity which means the IT dept would have to manage each one of them.

Security and Firmware Governance

Definition

The advanced security settings of printers' and MFPs' device firmware has evolved as the complexity of supporting apps grows and unique customer IT environments change. Printer device firmware is the program stored in a printer which allows it to receive information and turns it into a printed page, scanned image or sends alerts to replace toner. OEMs modify firmware occasionally for printers and MFPs (like PC and phone makers) which they then make available for official distribution with release notes.

Modified firmware can be updated as easily as sending a print job to a network printer or using a USB key. Firmware modification attacks have been demonstrated on HP, Canon and Xerox devices in the past. As a countermeasure, OEMs have implemented digitally signed firmware to help protect against malicious security attacks.

Organizations with complex printing requirements perform rigorous testing to ensure the printing technology supports key business applications and conforms with network security standards. This testing generally considers the device firmware as a certified version for the organization. Furthermore, this is important for government security certifications like the Federal Information Processing Standards (FIPS) 140 in the United States.

Considerations

Get Informed

Ensure you have complete knowledge on the firmware versions available for the portfolio of devices you offer. Each OEM has a different way of monitoring and managing these changes, including manual or automated methods. Understand how your team can be efficient in deploying necessary changes which may mean an upgrade or downgrade of firmware. Become familiar with the available tools from the OEMs to support a governance methodology for fleet firmware and security setting configurations.

Assess Customers for New Business

MPS organizations should consider offering a fleet assessment to get the full picture of the device firmware already in place for a customer's fleet of devices. The best advice is "if it ain't broke, don't fix it". Just because there is a new device firmware available, doesn't mean the services team should proactively update it. By updating firmware, something else may stop working like print management software or workflow processes.

Ongoing Governance

It is recommended to read the release notes and be familiar with a known 'golden' level of firmware to ensure the best performance and security for customers. The OEMs are actively making changes on how the devices operate and with different makes and models this becomes even more complex.

MPS organizations should be able to offer professional services to improve and maintain the security and performance of the fleet, but make sure thorough research is conducted before making security recommendations.

Benefits

Actively assessing new opportunities and existing fleets can help uncover new business opportunities. Organizations of all sizes are becoming more informed about the potential security exposures due to aging, unmanaged or unprotected fleets of printers and MFPs.

Understanding specific models of devices that lack digitally signed firmware is an easy way to identify new device replacement opportunities. Usually, if this feature is missing, there are additional security vulnerabilities of the fleet.

Also, by educating customers about the potential malicious security risks, you position your organization as a leader in information security. Thought leadership and differentiated security services can set your team apart from local or national competition.

Security and Firmware Governance for Remote Working

Governance starts with a well thought out plan. Unfortunately, the recent proliferation of consumer-grade devices and usage of old printers in home offices may have opened companies to security risks. MPS providers have the opportunity now to assess the remote office printer fleet landscape and to recommend the most appropriate devices and configurations to ensure security and firmware governance for MPS customers.

Service Engagement Policy

Definition

A proper service engagement policy is intended to ensure that the precautions and settings applied at the device level stay intact regardless of the service intervention required.

Considerations

Considerable time goes into developing precautionary protocols at the device level and the same consideration should be managed to by any service provider triaging or remediating a print device. Selecting a service provider that can manage existing protocols/settings is vital to the protection of an organization's data. A service provider that doesn't adhere or take steps to restore protocols can easily undo any precautions that were put into place as a result of earlier sections of this document. There also needs to be a security information and event management protocol in place to detect a failure to restore the proper protocol.

There is significant risk of exposure with minimal costs associated with this topic:

- Risk
    - Service Provider Compliance
    - Protocol Compliance
    - Setting Compliance
- Cost
    - Service Provider Selection
    - Security Information and Event Management

Areas of focus

- Selection of a service provider willing to adhere to protocols
- Consideration of inclusion in service contract
- The service provider is the first line to maintain desired protocols, however, there needs to be a proper SIEM in place to detect any failure

Benefits

Selection of a proper service provider will help maintain protocols that were determined necessary to protect an organization's network and data. In addition to selecting the proper service organization, there should be a security information and event management protocol in place to help identify any lapses. Selecting a competent service organization will not only increase up time but also help protect the organization's network.

Secure Document Disposal Services / Data Leak Protection

Definition

Secure Document Disposal and Data Leak/Loss Protection are two critical areas of protection around exposure points for sensitive information. Businesses exchange or collaborate daily on confidential information about their own organizations or their customer's businesses. The exposure of confidential data via printed or electronic documents is a serious threat to those businesses and can affect the livelihood or success of an organization.

According to IDC research reported in a 2015 white paper on "The Business Value of Printer Security", 80% of the companies surveyed indicated that IT security is important to their businesses, but only 59% of those companies stated that print security was important to the business. This points to the vulnerability to businesses who let their guard down around printed or electronic data. Furthermore, IDC found that half those businesses surveyed had experienced an IT security breach that included print security in the previous 12 months.

Data loss protection is the strategy for ensuring employees/end users do not send sensitive information outside the company network. Gartner, an industry research firm, uses their Magic Quadrant visualization approach around enterprise data loss protection, and the companies that focus on helping in this area.

Considerations

Consideration needs to be given to data access across both digital and physical methods. Digital methods may represent information that rests in your network, sent/stored outside your network, viewed on mobile devices, etc. Physical methods may represent information printed for specific use, but vulnerable to exposure/access outside that use. With the proliferation and exponential growth of IoT, end point devices represent a great threat to these critical areas.

The following best practices look at how you may protect sensitive documents and data. Although they are meant to be as comprehensive as possible based on where the Industry is in security, they are certain to be out of date at the rate this area is changing and adapting to new and creative ways people are accessing information. Providers are encouraged to have knowledgeable resources to stay current with changes and improvements.

Document & Data Policies

Establish business rules and policies around hard copy and electronic information access, use, management, and distribution. These should cover both hard copy and electronic documents. This is also often referred to as enterprise content management, or ECM. It is a set of defined processes, strategies, and tools that allow a business to effectively obtain, store, and deliver critical information to its employees, business stakeholders, and customers.

Areas to cover:

- End point devices, i.e. computers, cell phones, printers
- Electronic content management, i.e. storage, password protection, encryption, USB drives
- Access levels to sensitive information
- Document disposal

Education & Awareness

Establish content for new employees and ongoing training for existing employees that educate on vulnerability and impact that the loss of sensitive data could have on the business, and their responsibility to manage that data to the policies and procedures set by their company.

Management & Reporting

Incorporate systems and tools that allow for monitoring and reporting around any access, use, or violation of data policies. These should be constantly reviewed and escalated when there is any questionable exceptions or activity.

Benefits

Creating effective processes around protecting sensitive information across both digital and physical methods helps protect businesses and their customers from potentially catastrophic misuse of that data.

Secure Document Disposal and DLP for Remote Working

Printed pages from remote workers printing at home that are disposed of through their normal public sanitation is not a secure method of disposal. On the contrary, these documents are considered abandoned by most local/state laws and are deemed to be public property. Work with your customers to understand the sensitivity of the documents that remote workers could be printing at home to be able to offer secure document disposal services. For highly regulated customers, like those in healthcare, onsite services for the remote employees like shredders might be needed; others might require scheduled services where offsite disposal is acceptable.

Secure Device Disposal

Definition

Always ensure that a security policy takes into consideration all "areas of rest" that a document or information might follow in the journey of converting from digital to physical content. Putting this in the context of a device, it is appropriate to apply the "cradle to grave" methodology, where the device is correctly configured and deployed at the birth stage of the program and, in turn, is given deserved burial rights to remain compliant.

Considerations

There are numerous measures that can be taken regarding the secure disposal of devices. However, it all needs to be relevant to the level of risk associated with the device and the organization it is deployed within, and to the cost associated with the appropriate disposal.

As mentioned, the scale of risk versus cost needs to be weighed by each organization and their specific business or compliance requirements. The elements that would tip the scale on each of these elements include:

- Risk
    - PCI compliance
    - HIPAA compliance
    - Internal risk compliance
- Cost
    - HDD not sanitized / erased
    - HDD securely sanitized offsite (device refurbished and sold secondhand)
    - HDD securely sanitized onsite
    - HDD left with customer to destroy
    - HDD destroyed (shredded) onsite
    - HDD scrubbed and then destroyed onsite

Areas of Focus

- Clear address books
- Hard drive overwrites
- Nonvolatile RAM erased (Fax memory)
- Configurations reset to factory settings
- Removal of asset tags, queue paths, device names, etc.

Benefits

All the above have varying impact on the balance of the scale and the cost element runs from least costly (most risk) to most costly (least risk). It is the responsibility of the service provider to once again be the trusted advisor to their client and guide them in the most appropriate device disposal strategy; not be to champion profiteering within the account, but rather to propose a strategy which protects the client's data integrity at the most appropriate cost.

Secure Device Disposal for Remote Working

Device disposal processes may change during a pandemic. It would be best to schedule device removal, data sanitization and device sanitization for after hours to avoid technician / employee contact. Also, plan to utilize the web interface of devices to invoke the end of lease sanitization functions remotely prior to device power down and removal to minimize time at the device by technicians. Consider how devices associated with remote or home workers will be data sanitized prior to disposal.

Software

Definition

Software, in the context of managed print, refers to print device features, client printing software, and hosted print infrastructure. While not an exhaustive list, the following areas should be prioritized when considering securing the printing environment: data encryption, secure print release, print drivers, and cloud-hosted print solutions.

Considerations

Securing the software components of the solution can be challenging given the variety of vendors, products, and solutions that comprise the implementation, but with a reasonable amount of due diligence by the service provider, a security baseline of the offering portfolio can be established.

- Encryption: encryption should be evaluated for both data at rest and data in motion. To secure data at rest, full HDD encryption should be enabled. To secure data in motion, connections between the client, print/multifunction device, and scan repositories should be encrypted with a secure transport.
- Secure print release: this capability holds the print job at the device and requires authentication before the job is printed. Authentication can be in the form of a PIN, password, or physical card.
- Print drivers: print drivers routinely have access to the operating system at some level, so the following key considerations include:
    - Are the print driver supplier developer's trained in secure coding practices?
    - Have the print drivers been digitally signed by the provider?
    - Have the print drivers been scanned, and all vulnerabilities addressed before release?
    - Does the provider have a process in place to provide print driver updates on a regular basis?
- Cloud hosting solutions: print solutions should be hosted in professional, secure environments that provide redundancy or recovery capabilities. Key considerations include:
    - Does the hosting provider maintain industry standard security certifications such as SSA16, ISO27001, SOC 2, etc.?
    - Does the hosting provider offer redundancy or other mechanisms to ensure adequate solution availability?
    - Has the environment hosting the solution been configured to limit access to appropriate parties?
    - Have all connections to solution "back ends" been configured with secure transport such at TLS?
    - Has penetration testing been conducted against the environment?

Benefits

- Encryption: HDD encryption provides assurance that device settings, user authentication databases, job logs, and other data cannot be accessed if the HDD is removed, while encrypting data in motion ensures jobs cannot be intercepted, reconstructed, and printed by unauthorized individuals.
- Secure print release: requiring a PIN, password, or physical badge/card before releasing the job lessens the chance that unintended users will see or mistakenly (or not) remove the hardcopy.
- Print drivers: as software applications, vulnerable print drivers can lead to an exposure of the client, which then could be used as a launching point for other attacks.
- Cloud hosting solutions: securing the hosting environment will help ensure any printing or workflow solution will not be compromised and, by confirming provider recovery and uptime capabilities, will ensure contractual metrics are achieved for the services provided to the customer.

Software for Remote Working

Software solutions may help reduce touch points during a pandemic. Example: Device monitoring software can help predict failures and consumable needs to allow service technicians the opportunity to schedule and batch these activities during periods where there is less exposure to users.

Security and Compliance Assessment

Definition

Security in relationship to Managed Print Services strives to protect user and device data and prevent the interruption of print services. User (personal) data can be defined as data collected which can reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership, data for the processing of genetic data, etc. or any data that could identify directly or indirectly a natural person. It also includes access credentials e.g. passwords and cards, which authenticates a person to a device or service allowing access to secured data such as a document or device. Interruption of service can be defined as a denial of service to a legitimate user to access a device due to a security breach.

Security technologies used include encryption to protect data such as MFD hard drive and authentication to permit access to a device or service.

A compliance assessment should reveal the extent an organization protects its personal data and device assets. Full compliance ensures personal data and device access are secure.

Considerations

Understand the Organization

Fleshing out the security compliance requirements can depend on several factors. These factors are sometimes common among certain organizations and can be profiled. Among the factors that should be considered are the following:

- Organization type e.g. financial institution, government, education etc.
- Organization size e.g. small (1 to 250 employees), medium and enterprise
- IT structure (sec department) and whether the customer's users and IT assets are managed internally or externally
- Security policies e.g. do they qualify vendors, what data protections do they require, what processes do they follow

Typically, banks, financial services and government organizations have the strictest security compliance requirements. They may have the most complicated security procedures that entail the greatest understanding and process time. Other organizations such as industrial companies with no or limited security departments may require only basic compliance. In any case, profiling the organization identifies what security competencies are needed to offer the compliance assessment.

With respect to security policies, most organizations will have a security questionnaire to qualify new vendors and applications. Becoming familiar with these types of questionnaires and developing responses to them is a best practice which can enable dealers to quickly move a compliance assessment opportunity along. It also identifies the security sensitivities the organization may have regarding data protection and device accessibility. Other structure and policy factors to know include:

- What entity is responsible for security. Typically, it is the domain of the IT department, but it can be finance
- What management level reviews security and assigns access to services and devices
- What are the engineering change procedures and the duration for approval
- What are the key security threats and challenges of the organization

Customer Environment

Drilling down from the organization profile to learn about the actual customer environment is paramount. Scoping the compliance assessment will require knowledge about the specific software and hardware used in the environment. Some key environmental data points are:

- What is the current fleet mix, the MFDs, SFD, local printers and their assigned purpose, are there devices setup for secure printing
- What device management protection is currently in place, do they use SNMPv3 for fleet management
- What document management securities are in place, are card readers for follow me printing used etc.
- What inbound and outbound traffic is allowed; do they allow data to go out over the Internet
- What compliance certifications do they adhere to if any

It may be useful to know the specific software and hardware versions and models deployed as some may have known security threats. It is also important to understand the customer's processes for managing security. Do they have existing processes in place the dealer can piggyback on? Do they involve outside consultants or rely on internal security experts? The dealer will need to get to know the critical players that manage security.

Knowing the customer environment will assist in assessing what the threats are to the environment. For example, if a device is exposed to the Internet, it may be vulnerable to denial of service attacks. If data is stored on the hard drive of an MFD, it may be vulnerable to access by an illegitimate user.

Customer Deliverable – Risk Assessment and Services

Identifying the threats and vulnerabilities and recommended remedies in a compliance assessment report and/or presentation is a deliverable. Consideration to using a threat level metric such as high, medium and low for emphasis can help communicate the risk for the customer. Ultimately, the dealer is providing a risk assessment based on the specialized knowledge of the industry and MPS best practices. In addition to the risk assessment, the dealer can offer security services to deploy or repair the current service to meet the targeted security compliance as a follow-on deliverable.

Benefits

Professional Service Revenue

By offering security compliance assessments, the dealer opens the door to providing a critical service which can be highly profitable. This can be a new source of revenue that leverages the expertise the dealer has in the

print industry by combining a highly sought-after IT skill in security. Security experts are among the most highly paid IT professionals but often lack the knowledge and experience in print. This presents an opportunity for dealers to add a risk assessment and follow on security services to their professional services revenue.

Customer Loyalty

Dealers can build customer loyalty by being a mission critical supplier. Security is a mission critical process for most organizations and, to the degree the dealer involves their services with security, they can become indispensable to their customers.

Security and Compliance Assessment for Remote Working

Work from home use of printers pose additional exposure that the normal security practices and protections that exist in the office are not in place or followed at home. It is crucial to understand your organization's policies around data protection related to printers and ensure the guidelines and compliance measures listed by your organization are considered and followed.

Software Deployment / Secure Remote Management / Rights Management

Definition

Software deployment is the process of installing or running software without installation within the customer's firewall. Depending on the software application, it may be installed on a dedicated platform e.g. Windows or virtualized using VMware etc. and managed by the MPS provider or the target customer. Typically, a license enables the application's operation and fees are charged in advance of application use or based on a usage model (Software as a Service) and paid in arrears. Remote management is the process of utilizing that software application from outside the customer's firewall. Both processes should require some level of customer involvement i.e. approval prior to installation/running of software and remote use of the software. This may require a document review by the customer's IT security department or agency and/or participation of IT administration. Some testing as a proof of concept (PoC) is typically required in medium to large environments prior to production deployment.

A smooth and successful deployment, one with few implementation errors, can set the stage for a positive relationship with the customer.

Considerations

Understand the Customer's Organization

Deployment Perquisites - prerequisites to deploy software varies based the customer organization type and size. These prerequisites often include the following:

- Software documentation which describes how the software is deployed and operates
  + Hardware and software requirements e.g. processor speed and Windows platform
  + Network traffic
  + Network protocols
  + Security and Access control (Whitepaper)
- Telco with customer IT department
  + Security/database (dba) and network representatives
  + Review deployment requirements
  + Determine what customer assistance is required
    - Hardware
    - Database access
    - User authentication
  + Deployment milestones and schedule
- Customer approval to deploy
  + Verbal or by agreement
- Organization size by employees
  + Verbal or by agreement
    - Large >1,500:
      - mitigate delays with upfront 'buy-ins' from multiple departments and stakeholders

        - designate lead technical and communication person(s)
        - find out established deployment and change process
        - maintain constant communications ideally face-to-face meetings
        - remote management may be limited or prohibited by security policy
- Medium 250 to 1,500:
    - customer communication typically limited to 1 or 2 key IT people
    - deployment approval focused on IT resource availability and security check
    - remote management is typically allowed after security approval

- Small <250:
    - typically, a deployment can be organized quickly and fewer approval levels
    - some cases outside IT agencies are involved with setup
    - very small organizations hardware resources are limited and deployment can be with an office manager or secretary on a machine which it turned off at night

Organization type is another critical consideration particularly concerning security. The selection of the solution may depend on the organization's security limitations. Financial and public sector organizations are sensitive to data being exposed to the Internet. Other organizations such as retail, industrial and travel are not as sensitive and Cloud solutions are fine to deployment.

In summary, key items to consider when deploying software and providing remote management access are:

- Organization size
- Organization type
- Security and networking limitations
- Customer IT staff availability and capabilities
- Customer approval process
- Overall cost of deployment in terms of time and license

Benefits

Professional Service Revenue

By offering deployment services, the dealer opens the door to providing a first impression of the dealer's technical and customer care capabilities. Smooth and uneventful installations build confidence in the relationship.

For large installations, dealers may quote an installation fee, a new source of revenue that leverages the expertise the dealer has. This presents an opportunity for dealers to add deployment services to their professional service revenue.

Remote management allows the dealer to know of a problem before the customer knows. It also allows the dealer to lower costs by reducing the number of customer trips.

Customer Loyalty

Dealers can build customer loyalty by being a mission critical supplier. Deployment and remote management are critical processes for most organizations and, to the degree the dealer involves their services with the security, they can become indispensable to their customers.

Software Deployment / Secure Remote Management / Rights Management for Remote Working

Remote software deployment has been acceptable for many years now and during this pandemic it is the preferred method of software/ firmware installation services. When performing these services, ensure that tools to perform this work securely without compromising your customers network infrastructure are available. Always make sure your customer is present for accepting all EULAs or have in writing that you can accept EULAs on their behalf.

Secure Pull Printing

Definition

Pull printing, known as secure release / pull printing, allows users to securely print while moving around the office or even across locations. Documents are held by a server or workstation and are only sent to be printed when the user has authenticated themselves by typing in a PIN, username/password or tapped their ID badge at the device. Generally, staff can print all the documents in their personal queue or select specific print jobs to print or delete from any appropriately configured device on the network.

As print jobs do not print until the user is at the device, documents remain protected with pull printing technology. The product can be configured to print between floors, buildings or different locations, allowing staff to print securely wherever they work. All documents printed via the secure print queue are encrypted by the software to ensure secure transit from workstation, to server and eventually produced on the device. Printing from smart phones and tablets is also possible but may require additional software from the vendor or another solution.

Pull printing technology has been available for over 20 years but has been broadly adopted over the past 10 years with leading independent software vendors. There are multiple independent software vendors who provide multi-vendor solution support which is necessary for most MPS providers, as very few ecosystems have a single vendor deployment. OEM vendors have started offering their own pull print solutions in the past five years.

By implementing a secure pull print solution, the provider can showcase to their clients the who, where and what of printing. Because the software collect all the metadata (user, document name, application, page count, etc.) associated with all jobs, it allows the reseller provide a consultative view into the customers printing habits and suggest data supported guidance on how the environment could be better managed.

With data supported visibility on printing habits, rules can be implemented to control what documents may or may not be printed, based on the customer's specific requirements. These rules can lead to security compliance as well as potential savings for the business.

Considerations

Where to look

It is advantageous to consider secure pull printing as a standard part of a managed print services contract. This is incremental revenue and added value to the customer to improve security, avoid waste and facilitate employee productivity. A visit to the client's office can immediately uncover the need for pull printing by looking for documents sitting in the output tray of printers and MFPs.

An office visit should:

- Help identify paper documents and departments currently at risk
- Reveal existing practices or solutions in place to secure documents
- Uncover if the existing solution and service meets the client's future needs

Where to turn
As this is a mature solution segment, it is recommended to reach out to the experts. Identify the leading vendors that are compatible with the MPS fleet offering. Review and compare the available software test reports from independent test labs such as Buyers Laboratory Inc. (BLI).

Each pull print vendor has an industry vertical specialization. Several vendors started in the education market, others have been established for commercial and public sector markets.

Where to start
MPS providers should determine if they have the appropriate services staff to sell and deploy pull printing solutions. If they do, the professional services staff can immediately start training and offer the solution to customers directly. If they don't, the software vendors and their distributors will be able to assist in the presales and implementation for clients.

Benefits

More Revenue but Increased Security

It is highly likely that organizations have experienced a data breach due to printing. Quocirca reported in 2017 that 61% of medium to large organizations have reported an occurrence due to un-secure paper-based processes. Visiting the customer's location provides essential information about potential revenue opportunity for MPS providers and potential security risk for the client. Per Gartner, revenue for solutions like pull printing can represent up to 10% of the MPS deal.

Stickiness

Once clients start using secure pull printing solutions successfully, it is difficult to unseat the MPS solution provider. The flexibility it gives to staff, plus the security and cost control it provides to management, make it a game changer. Renewal rates for MPS accounts with secure pull printing are very high.

Secure Pull Printing for Remote Working

Investigating printing bottlenecks with MPS customers may reveal business continuity situations when printing from corporate business systems by remote workers. If business critical processes require documents to be printed in the office environment, print management software can be configured to enable printing securely on premise, without remote workers leaving their home office. Most pull printing solutions have shared team or delegated printing features to enable secure printing at the corporate office by a designed staff member(s) to continue business critical processes.

Secure Workflow

Definition

The following few sections in most cases are overlooked by resellers due to the complexity of the engagement required; this makes for high risk to the organization. Understanding and mapping the path of data is critical to ensuring it remains secure.

In the simplest of terms, it's all about knowing the path data takes to get from point A to point B and how do you, as the service provider, ensure it takes the safest route. Similar to a presidential motorcade on a route, it is plotted with precision to ensure minimal stops along the route, if any, with guards in the vehicle, support vehicles with teams in them surrounding the president's vehicle, and police motorcycles blocking various adjoining roads to ensure no interference. In some people's eyes, it may feel like a complete overkill and a waste of money and resources given the likelihood that something will happen. However, it only takes once for a catastrophe to hit.

Secured workflow takes the discussion from mere control of the amount or sensitivity of data being produced on a paper medium to where is it derived from, who are the approved users for access, where is it stored, and how can it be shared.

Considerations

There are multiple layers to consider when reviewing the workflow of an environment. Start with ensuring that the appropriate guidelines are implemented to achieve a structured design, a blueprint essentially. From this foundation, build out the strategy and ensure the necessary support is gained at each level. As with everything in life, have a plan and let others know and understand your plan.

- Governance

  At a corporate level, it is key to understand the expectations and policies needed to be supported for the organization. There may be elements that are not standard in how they need their data route controlled, which needs to be taken into consideration.

  Consider legislative compliance within the specific market the organization conducts business. As one example, if they are in healthcare, there is the need to remain HIPAA compliant with regards to patients' personal health information. If this data is leaked, there are serious consequences.

- File Encryption

  The workflow of a document cannot be secured unless the file is encrypted, and the path controlled from end to end. The starting point is as important as the destination and what happens with the information when it has transferred successfully. To achieve this, there needs to be a trusted source and trusted destination (relationship) along the path which the data travels.

- User Knowledge

  If anything is to remain secure, it is fundamentally reliant on the understanding and support of all people involved in the process. Your security architecture is only as strong as the weakest link, therefore, user training and an understanding of why the security measures are in place and what effect it may have if they don't support it, is key for success. This training should reinforced on a continuous basis.

Benefits

Securing the workflow of data has many codependences with the rest of the environment as covered in this white paper, however, if done synergistically, it will ensure the protection of the environment's data, along whichever path it is required to take. This in turn relates back to the service provider having to intervene less, should there be any expected data breach of a document through the print infrastructure.

If system health is maintained and an audit trail or compliance report is logged and made available, the service provider can allow the client to continue with their breach investigation knowing that the print environment was not the point of failure. At the same time, the service provider can potentially further assist the client through contracted services to ascertain why the breach occurred.

Secure Workflow for Remote Working

It is recommended to identify business workflows that might be impeded or broken when moving workers to home offices or other remote locations. Once identified, digital ways of working may be available to implement immediately by converting documents to PDFs and sharing them in a cloud-based repository for additional processing.

Additional software solutions are available to fully automate and streamline these workflows and customers will be looking to redesign business critical workflows for employees no matter where they work. For resellers looking for new revenue streams as page volumes are in flux, secure workflow solutions are area to investigate immediately.

Print Drivers

Definition

Print driver management has become more of a requirement to be fulfilled by the MPS provider and less that of the customer's IT department. The reason for this is that print drivers are changing as quickly as Microsoft patch updates and keeping up to date on all the drivers can be an onerous task.

If drivers are not kept up to date and in sync with the operating system standard on the client, there could be system conflicts, errors and security risks. This can cause the environment to fail and users may not be able to print. In some cases, this becomes more of a mission critical support aspect than e-mail for the customer's IT, as their help desk is bombarded with support requests.

Therefore, it is critical for the MPS provider to review and test all driver updates published by the vendor which pertain to the fleets they are supporting across their customer environments.

Considerations

Some of the elements to consider include the adoption of a universal print driver. If there is a single brand fleet in the customer environment, it is more effective to have a single driver available for deployment which supports all application, finishing and format requirements. If there is a mixed fleet, a universal print driver can effectively manage the basic print functionality but will most likely struggle with advanced finishing like stapling, offset, etc.

When very specific and advanced finishing functionality is available at the device level and users are in fact utilizing the tools, it is advised that a vendor specific universal print driver be used. In a few isolated cases, it may be better to install the device specific driver for full functionality integration and utilization.

It is also recommended for security and ease of support, that print queues be implemented at a print server level. This ensures that the correct driver is installed across the environment to all workstations. By configuring the MFPs' and printers' allowed communication channels (IP Authorization), users will only be able to print to the devices via the print server which ensures no rogue drivers and potential hack conduits enter the customer ecosystem.

Benefits

If print drivers are maintained effectively, it leads to customers having better availability of their print environment and less risk on their business processes.

Use of a Universal Print Driver allows for far less support and maintenance in rolling out updated versions to the user community and environment, as the print server queue can be updated with the latest driver version, which will update each deployment.

Secure Pull Printing for Remote Working

Depending on the security policies and permissions granted for staff, remote workers may not be able to install print drivers for home office printers to easily print when needed. This may open unnecessary risks as end users look for other ways to print company documents at the home office, work around digital rights management controls and expos companies to security risks. Make sure to incorporate questions for MPS customers about this potential risk in a Remote Working Assessment.

Cloud Print / Apps

Definition

The digital transformation of the modern workplace is at full speed and not showing any signs of slowing down. With technology making it much simpler for the user to conduct all their business activities outside of any company building and being "off the grid" when it comes to the corporate network, it is imperative to change the way we architect the print environment.

Print certainly still has its place in the business world and, even though statistics show print volume is on a decline, the decline is very slight with no dramatic drop-off. This, combined with hardware manufacturers showing growth in their segment sales, is testament to the fact that businesses need effective printing solutions and are invariably upgrading to benefit from the lower running costs as well as security compliance of the newer technologies.

Considerations

With office productivity tools becoming cloud and subscription-based models, it dictates a review on how and what users require to fulfill their business roles. The table below provides a high-level comparison between the two primary mainstream product suites and it is more than clear that the direction is cloud.

Capability	Google Apps	Google Apps	Office 365	Office 365	Office 365	Office 365	Office 365
Product edition	Basic	w/vault	Personal	Home	Bus. Essentials	Bus. Premium	Enterprise E3
Email	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Video conferencing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Social Network	Yes (G+)	Yes (G+)			Yes	Yes	Yes
Calendar	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Word processor	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Spreadsheet	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Presentation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile apps	Yes	Yes	Yes	Yes		Yes	Yes
Installable desktop apps			Yes	Yes		Yes	Yes
Storage	30GB	unlimited	1TB	1TB/user	1TB/user	1TB/user	1TB/user

Table courtesy: David Gewirtz of DIY-IT

With this in mind, what do MPS providers need to do to remain relevant in the current technology landscape and what service do they need to provide that supports the needs of a workforce that are becoming more remote? By leveraging new technology offered by software providers, we as solution providers can better position ourselves as Value-Added Service Providers when incorporating these elements holistically. There is high demand for common repeatable functions in business to be automated and streamlined. This topic moves into the realm of Business Process Engineering and a topic for another white paper. It is worth considering how to embrace technology and the aggressive growth instead of fighting it and potentially falling victim to it surpassing your offerings.

Therefore, MPS providers need to consider how to provide solutions that enable all users, based anywhere in the world, at any time/time zone, in any language that have the infrastructure and support customers expect while conforming to IT security governance. With the IoT and cloud-based-anything nowadays, this is certainly possible, feasible and, in a many ways, makes perfect sense for where the world is headed with regards to a smarter digital workforce.

There are key tools you need in your toolbox to support such an environment:

- Enterprise grade print queue and driver management system. There are many available in the market today, but it is key to ensure you consider the expectations of your clients regarding the following:
    - Security compliance
    - Distributed workforce percentage of the total compliment
    - Print queue management deployment (usage tracking, policy deployment/enforcement
    - Hardware extended functionality requirements as this becomes challenging when disparate vendor equipment has been deployed in the environment (stapling, etc.)
- Remote device support capability
    - Devices to be networked for remote troubleshooting
    - Remote desktop session capability
    - Device health tracking for pro-active remote support
- Cloud deployment
    - Self-service print queue install functionality based on current location of roaming user
- Mobile print capability
    - Mobile device integration to cloud print queue solution (usage tracking)
    - Consider complexity of wireless network printing versus peer-to-peer and user support for both based on an invariable scenario of there being a multitude of basic home network configurations

Benefits

The clear benefit of incorporating the mobile workforce environment and providing a cloud-based solution that supports app centric future architecture ensures a dealer can remain relevant to the customer, removing the burden of their IT department having to design an appropriate and industry best practice aligned solution.

The reality of all IT departments is that they have far more important elements they need to support in the environment; the print ecosystem is certainly the last on their list of demanding tasks to complete. Yet, when we evaluate the composition service desk tickets, we find anywhere from 10% to 25% are print issue related. This in turn makes it a painful enough element to ensure that the architecture is designed in a manner which supports self-service by the end user but maintains a stability standard that ensures little to no IT support engagement.

Cloud Print / Apps for Remote Working

Enabling home office printers with cloud printing and other apps will be dependent on the range of devices they use. No two manufacturers provide the same capabilities and your team may be challenged to find apps to support the disparate fleet of inkjet and laser products in the WFH environment.

It is recommended to assess the needs of the WFH users first and then recommend a WFH platform with the choice of productivity apps that you are ready support. These apps don't have to be free, as you are providing additional services beyond buying a printer and supplies like Amazon.

Security Reporting and Review

Definition

Security reporting tools can provide data to track all print, copy, fax, scan and email activity across the entire organization and manage security configuration and firmware of the fleet. These reporting activities are generally spread across multiple network applications, from independent software vendors (ISVs) and directly from the OEM vendors.

Reporting tools can include a set of basic reporting templates and the ability to create customized on-demand reports to meet any unique organizational need. Reports can be scheduled to automatically send via e-mail or saved to be accessed online.

Advanced security reporting can also be implemented when monitoring the content being printed, scanned or faxed, such as account numbers, credit card numbers or keywords in the body of documents. For organizations focused on data protection regulations, this advanced security reporting could be a key requirement.

Considerations

Consider the portfolio of products you sell and the tools available for security reporting. The services team will need to understand the best combination of tools to proactively report on the fleet in order to be prepared for monthly or quarterly meetings with the client.

Understand what your existing and prospective customers are most concerned about in relation to securing documents to communicate with them about potential security breaches. Use the outputs from the reporting tools to identify opportunities to continuously improve their environment and differentiate your consultancy services.

Benefits

There are many business benefits of leveraging security reporting and reviews:

1. A complete understanding of your client's environment (managed and unmanaged) for future business
2. Providing proactive services to keep the client's environment manageable and secure
3. Articulating the value your company is providing in management reviews

The sales and operations teams will need to work together to incorporate the security reporting details into an integrated communication to the customer including technical and commercial aspects.

Security Reporting and Review for Remote Working

Work from home use of printers often means you do not have the same reporting tools and review processes in place that you have in an office environment. One option is to download additional free management software made available by the majority of printer OEM's to assist in this area. These management tools (HP - Web JetAdmin, Lexmark - MarkVision, etc.) offer the ability to set, manage, and report on key variables crucial to reporting on device usage and security.

Appoint a Champion

A final recommendation is to appoint a "champion" to ensure the MPS provider implements, adheres to, and improves processes that enhance profitability and customer satisfaction in security management. This champion could be a single person or a task force that meets regularly to review issues and corrective actions. Regardless of the configuration the provider chooses, success will mirror focus and commitment.

Conclusion

The best practices around the security of a print environment included in this document are intended to protect an organization's print environment from an internal or external data breach. In evaluating any of these best practices, one must take into consideration the needs of the organization. Those factors include the cost to implement the practice, potential impacts the practice could have on an organization's workflow and the overall risk assessment of an organization.

As with the implementation of any new protocol, much of the effectiveness of the measures implemented greatly depend on user adoption. There should be a strong consideration given to necessary changes in user behavior under these new protocols. There should be a change management plan implemented with importance placed on the sense of urgency that surrounds the security of the print environment.

These best practices are suggested to help minimize a dealer's cost exposure and improve customer experience. They offer you – the MPS practitioner – an opportunity to promote overall profitability and create ongoing value in your company and for your customers. Ultimately, the success of your MPS program will rely upon how you choose to apply these considerations throughout the entire lifecycle of your own MPS program.

As with all information, you must determine whether these best practices apply to your specific situation. Therefore, we encourage you to consider these best practices as part of the entire body of knowledge made available through the MPSA.

About the Standards and Best Practices Committee

MPSA Standards and Best Practices Committee Charter: In pursuit of excellence in the MPS industry and the customers served, the MPSA Standards and Best Practices Committee will define industry standards and best practices. This includes the organization, its committees and membership, as well as publishing standards and best practices for broader industry adoption.

Call to Join the Cause

The Standards and Best Practices Committee was one of the first MPSA committees founded in 2009. The committee has a history of producing quality outputs from some of the Industry's most experienced leaders.

If you are interested in joining this committee or contributing to make our association and industry better, please reach out to info@yourmpsa.org.