Technical white paper

Meet compliance requirements for network and data security

Recommendations for applying security controls to the printing fleet

Table of contents

Click here to verify the latest version of this document

Compliance infringement can hurt your business

In addition to expensive fines and lawsuits, a security breach can result in loss of revenue and a damaged reputation. When creating your security plan, remember your network is only as secure as your weakest link. Printing and imaging devices have many of the same security vulnerabilities as PCs. It's crucial to deploy devices and solutions that help you meet compliance requirements and protect your business information from security threats.

What's the risk?

Regulatory and legal noncompliance are resulting in heavy costs for global organisations including fines, lost business, damaged reputations, and class-action lawsuits.

Unprotected or under-protected endpoints create more opportunity for cybercrime. Organisations surveyed by Ponemon for a recent study experienced on average two attacks per week in 2016, an increase of 23% year on year, losing on average $9.5 million annually in the fight against cyber crime.[1] And last year alone, over 4 billion data records were compromised worldwide, a 400% increase over the previous two years.[2]

Although many IT departments rigorously apply security measures to computers and the network, printing and imaging devices are often overlooked. But printers can provide an entry to your network, and securing them is just as important. Of all significant data breaches reported by IT managers, 26% involved their printers.[3]

Utilise common security controls to improve compliance

It's challenging to keep up with industry compliance and regulations. Fortunately, the Center for Internet Security (CIS) has created a set of common security controls to simplify cybersecurity recommendations. The CIS Critical Security Controls are 20 specific actions that can help stop cyberattacks. (For details, see https://www.cisecurity.org/critical-controls.cfm.) The Controls align with many other industry regulations, such as PCI-DSS, ISO 27001, US CERT recommendations, HIPAA, FFIEC, and NIST. The Controls don't try to replace these other frameworks, but they are frequently used by enterprises to make sense of other frameworks.

The CIS Critical Security Controls prioritise a smaller number of actions with high pay-off results. They address the most common attack patterns from leading threat reports. A broad group of industry experts—including some of the top forensics and incident response organisations—helped create them. Plus, the Controls are continually updated based on evolving threats and attacks.

Use the CIS Critical Security Controls to help organise your security action plan and meet compliance regulations. This white paper provides suggested actions for each of the 20 Controls to help secure your print devices, data, and documents as part of your larger security plan.

CIS Critical Security Controls and recommended actions

CSC 1: Inventory of Authorised and Unauthorised Devices

Control—Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.

Recommendation—Ensure that all printing devices on the network are accounted for and actively managed for compliance with your security policy. An effective print security management tool can discover and supply visibility to all network and PC-connected devices.

CSC 2: Inventory of Authorised and Unauthorised Software

Control—Actively manage (inventory, track, and correct) all software on the network so that only authorised software is installed and can execute, and unauthorised and unmanaged software is found and prevented from installation or execution.

Recommendation—Make sure all firmware and solutions loaded onto printing and imaging devices are up-to-date, signed, and validated to be authentic. Choose print devices with built-in protection for BIOS and firmware to ensure only authentic code is loaded. Proactive firmware updates can be pushed across the fleet with print fleet management solutions. Software (server-based and client-based) should be signed and validated as authentic.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Control—Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Recommendation—Just like other network endpoints, printers should be configured securely. You should create and deploy a security policy across all of your printing devices and actively remediate any deviations from that policy. Security checklists (such as NIST) or security advisory services can help you design and deploy a comprehensive print security policy. An effective print security management tool can automate policy creation, deployment, assessment, and remediation of device settings across the print fleet. Enterprise-level multifunction printers (MFPs) have more than 250 security settings, so automating this process can save significant time.

CSC 4: Continuous Vulnerability Assessment and Remediation

Control—Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimise the window of opportunity for attackers.

Recommendation—Security Information and Event Management (SIEM) solutions such as ArcSight, Splunk or SIEMonster can monitor activity on your network in real time and notify administrators when incidents occur. It's just as important to monitor print devices as PCs—make sure your printers can send event syslog messages to your SIEM tool.

Choose print devices with features that can detect attacks in real time and automatically recover, to maximise uptime while minimising IT interventions.

To reduce vulnerabilities, use a fleet security management tool that can identify new printers and automatically apply your corporate security policy settings as soon as devices are connected to the network. Schedule regular assessments/remediations to keep the entire print fleet in compliance with policy.

CSC 5: Controlled Use of Administrative Privileges

Control—Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Recommendation—Choose print devices and solutions with the ability to authenticate users and control access to functionality based on a person's role, so only IT staff or other authorised personnel can set up and configure device settings. Use fleet security management software to deploy administrator passwords across the fleet.

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

Control—Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.

Recommendation—Print devices should have the ability to generate incident syslog messages, so your security team can regularly review audit logs to discover and resolve issues. Choose devices that can send these messages to fleet security management solutions and SIEM tools for both real-time monitoring and the ability to generate reports for audits or other compliance requirements.

CSC 7: Email and Web Browser Protections

Control—Minimise the attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems.

Recommendation—MFPs are often connected to the internet so, for example, they can send scans via email. Ensure emailed scans are encrypted to protect sensitive data. Deploy devices and solutions that can authenticate users and control access to resources within the device (such as web servers or email functionality) based on a person's role. Create a "Trusted Sites" list for your MFPs and manage this appropriately to ensure only trusted websites are accessed from the device. Integrate various authentication methods (such as PIN/PIC, LDAP, or Kerberos authentication) with Active Directory for streamlined management and increased security. Print devices that are connected to the network should have built-in malware and virus protection, and printer firmware should be regularly updated so the latest protections are in effect.

CSC 8: Malware Defenses

Control—Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Recommendation—Choose print devices that will load only verified, signed code and that have built-in anti-malware features to actively monitor device memory and reboot in the case of an attack. An effective print security management tool can automatically assess and remediate device settings across the fleet. You should also ensure that all print software solutions are signed and validated as authentic.

CSC 9: Limitation and Control of Network Ports, Protocols, and Services

Control—Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimise windows of vulnerability available to attackers.

Recommendation—If not already disabled by default, disable unused ports and unsecured protocols (such as FTP or Telnet) that attackers may use to access the device. Save IT time and reduce risk by deploying a print security management tool to automatically keep device settings compliant across the fleet. Use admin passwords, authentication, and role-based access controls to limit access to device functionality and settings.

CSC 10: Data Recovery Capability

Control—Properly back up critical information with a proven methodology for timely recovery.

Recommendation—This Control does not currently apply to printers.

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Control—Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Recommendation—Printers reside on the network and, just like other endpoints, they should be configured securely. An effective print security management tool can automate the deployment, assessment, and remediation of device settings across the fleet to help keep the network secure—while saving IT time.

CSC 12: Boundary Defense

Control—Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Recommendation—Use encryption to protect data in transit (print or scan jobs travelling to or from the printer) and at rest on the device hard drive. Choose print devices and solutions with the ability to authenticate users and control access to functionality based on a person's role so, for example, only authorised users can email scan jobs or send files to cloud destinations. Configure trusted websites in the "Trusted Sites" list on the device to prevent access to malicious websites. Secure mobile printing solutions can make it easy for users to print from their mobile devices while also protecting the network.

CSC 13: Data Protection

Control—Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Recommendation—Use encryption to protect data in transit (print or scan jobs travelling to or from the printer) and at rest on the device hard drive. Deploy pull print solutions to avoid having sensitive documents abandoned in output trays. Make sure data stored on device hard drives is securely erased before returning leased devices or recycling them at end-of-life.

CSC 14: Controlled Access Based on the Need to Know

Control—Track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Recommendation—Choose print devices and solutions with the ability to authenticate users and control access to functionality based on a person's role. Integrate various authentication methods (such as PIN/PIC, LDAP, or Kerberos authentication) with Active Directory for streamlined management and increased security. Pull print solutions can protect sensitive documents from getting into the wrong hands.

CSC 15: Wireless Access Control

Control—Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

Recommendation—An effective print security management tool can automate the deployment, assessment, and remediation of device settings—including wireless settings—across the fleet. Use access control solutions to restrict access to device functionality, such as scan to email, based on the user's role. Secure mobile printing solutions can make it easy for users to print from their mobile devices while also protecting the network. For example, devices that support peer-to-peer wireless printing allow mobile device users to print directly to a printer's discrete wireless signal—without accessing the company network or wireless service.

CSC 16: Account Monitoring and Control

Control—Actively manage the life-cycle of system and application accounts—their creation, use, dormancy, deletion—in order to minimise opportunities for attackers to leverage them.

Recommendation—Choose print devices and solutions with the ability to authenticate users and control access to functionality based on a person's role. Integrate authentication with Active Directory for centralised management and increased security. Regularly review user accounts and disable unnecessary ones, and use tracking solutions to monitor account usage. Encrypt account usernames and authentication credentials, both in transit and at rest on device storage. Security consultants can help you design a comprehensive print security plan to help minimise risks—and in some cases, can help you manage security, including account monitoring and control.

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

Control—Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organisational planning, training, and awareness programmes for all functional roles in the organisation.

Recommendation—Print security consultants have the specialised knowledge to help you assess your security risks, develop a comprehensive security policy and plan, and implement process and technology recommendations. Some security services can even manage print security and compliance for you.

CSC 18: Application Software Security

Control—Manage the security life-cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Recommendation—Adhere to secure development best practices for all developed print solutions. Choose software solutions that have been signed and validated as authentic.

CSC 19: Incident Response and Management

Control—Protect the organisation's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight).

Recommendation—Confirm that your print environment is considered in your incident response plan.

CSC 20: Penetration Tests and Red Team Exercises

Control—Test the overall strength of an organisation's defenses (technology, processes, and people) by simulating the objectives and actions of an attacker.

Recommendation—Include your print environment when running penetration tests. Regularly assess your print environment for vulnerabilities and update your security plan to address these weaknesses.

Take the next step

Implementing the recommendations in this white paper can help you harden print security and meet compliance regulations. Need help? Print security management and advisory services can help you develop a plan and deploy processes and technology to improve the security of your print devices, data, and documents.

Appendix A: HP print security features, solutions, and services

The security features built into HP devices, along with industry-leading software solutions and services, can help you meet regulatory and legal compliance requirements and protect your business information from security threats.

Embedded security features in HP Enterprise printers and MFPs defend against malware and can automatically detect and recover from an attack. Only HP print security offers real-time detection, automated monitoring, and built-in software validation to stop threats the moment they start.[4] (Helps meet CSC 2, 4, 6, and 8.) hp.com/go/PrintersThatProtect

HP Access Control solutions provide a variety of authentication and role-based access controls to help reduce potential security breaches, plus job tracking and accounting. (Helps meet CSC 5, 7, 10, 12, 13, 14, 15, and 16.) hp.com/go/hpac

Encryption and **HP JetAdvantage Workflow Solutions** protect data both when it's stored on HP Enterprise devices and while it's travelling to or from printing devices or the cloud. (Helps meet CSC 12 and 13.) hp.com/go/upd, hp.com/go/documentmanagement

HP pull printing solutions protect confidential documents by storing print jobs on a protected server, in the cloud, or on your PC. Users authenticate at their chosen print location to pull and print their jobs. (Helps meet CSC 10, 13, and 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect gives mobile users easy access to printing from smart phones and tablets while maintaining the security and administrative control you need. (Helps meet CSC 12 and 15.) hp.com/go/JetAdvantageConnect

HP printer event data can be sent to SIEM tools, such as ArcSight, Splunk, or SIEMonster. Your security team can easily view printer endpoints as part of the broader IT ecosystem and can take corrective actions. (Helps meet CSC 4 and 6.)

HP JetAdvantage Security Manager is the industry's only policy-based print security compliance tool.[5] It helps you establish a fleet-wide security policy, automate device settings remediation, and install and renew unique certificates while getting the reports you need to prove compliance. The solution's Instant-On feature automatically configures new devices when they are added to the network or after a reboot. (Helps meet CSC 1, 2, 3, 4, 5, 6, 8, 9, 11, and 15.) hp.com/go/securitymanager

HP Secure Managed Print Services provides the strongest, most comprehensive print security protections in the industry.[6] Print security can be complicated. Let HP manage your print security from device hardening to advanced security solutions that address people, processes, and compliance requirements. (Helps meet CSC 2, 3, 12, 16, 17, 18, and 19.) hp.com/go/SecureMPS

HP Print Security Professional Services provide security experts to help you assess your print environment, proactively establish security policies, and keep your security plan up-to-date. We can even manage print security compliance for you. (Helps meet CSC 2, 3, 12, 16, 17, and 19.) hp.com/go/SecureMPS

Notes

[1] Ponemon Study sponsored by HPE "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 2016.

[2] The 2016 Year End Data Breach QuickView report by RiskBased Security, January 2017.

[3] 26.2% of survey respondents experienced a significant IT security breach that required remediation, and more than 26.1% of these incidents involved print. IDC, "IT and Print Security Survey 2015" IDC #US40612015, September, 2015.

[4] Applies to HP Enterprise-class devices introduced beginning in 2015 and is based on HP review of 2016 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. A FutureSmart service pack update may be required to activate security features. For a list of compatible products, visit hp.com/go/PrintersThatProtect. For more information, visit hp.com/go/printersecurityclaims.

[5] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager. Competitive claim based on HP internal research on competitor offerings (Device Security Comparison, January 2015) and Solutions Report on HP JetAdvantage Security Manager 2.1 from Buyers Laboratory LLC, February 2015.

[6] Includes device, data and document security capabilities by leading managed print service providers. Based on HP review of 2015-2016 publicly available information on security services, security and management software and device embedded security features of their competitive in-class printers. For more information, visit hp.com/go/MPSsecurityclaims or hp.com/go/mps.

4AA6-8821EEW, June 2017, Rev. 1