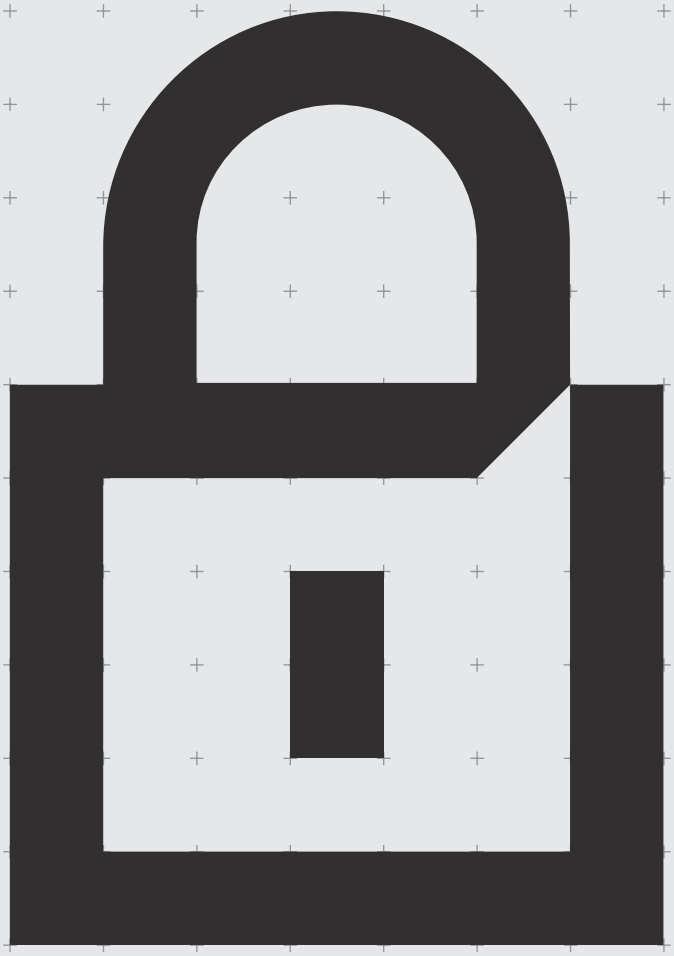
KYOCERA

kyoceradocumentsolutions.com

How to implement a successful print security strategy.



A practical guide for ensuring your print assets are never a cybersecurity liability.

When it comes to risk and reward, ongoing advances in digital technology are a double-edged sword. While the increasing influence of cloud IT, the Internet of Things and digital transformation each signify opportunities for business enablement, they also underline the need to secure all IP-connected print devices against both malicious cyber attacks and accidental data loss.

This eBook provides business leaders with a plan for developing and implementing a structured approach to secure their print assets.

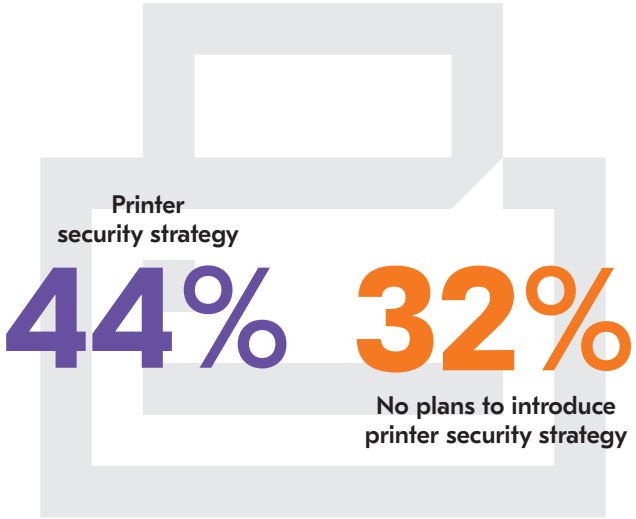
The scale of the issue.

Recent studies into the challenge of securing print devices, and the data they use, reveal that there is more to be done to ensure the appropriate protections are in place to counter both fundamental threat vectors and more advanced exploits.

Shortcomings in implementation of policy

Kyocera's research[1] into the cyber readiness of organisations shows that — when it comes to their current print and multifunctional device management solutions — enterprise decision makers are more concerned with prioritising lower costs (82%) and greater ease of use (60%) than addressing security concerns around access and data sharing (55%).

This is borne out in the finding that only 44% of organisations sampled have a print security strategy in place, and a further 32% have no plans to introduce one.



Looking closely at the security measures employed, there are signs that some strategic elements are widely evidenced. For instance, 76% stated they had a policy in place regarding the secure use of USB/external hard drives. However, only 40% could confidently say that this covered the use of printing via multifunction printer (MFP) devices. In terms of securing MFP hard drives, only 28% said that these were encrypted, while 38% said they employed a 'follow-me' print solution.

The indications are that enterprises are broadly cognisant of the challenges and risks of print security, but have the greatest difficulty in implementing a plan rather than developing a strategy.

Print security breaches — a clear & present danger

Perhaps the most arresting statistic from the Kyocera research is that around one in 12 respondents (8%) reported experiencing a print-related security breach. This is a large proportion given the relatively low public awareness of this issue, and places the potential impacts of revenue loss, compliance failure, business disruption and regulatory fines into the appropriate context.

Print security has begun to rise up the business agenda amid reports of the PewDiePie hacking scandal that specifically targets and controls print devices — bringing to reality what were once only theoretical capabilities.

The hundreds of thousands of printers involved in the latest waves of this attack escaped comparatively unscathed as the hacker's motive was to create publicity rather than commercial gain or malicious damage — both of which could have been eminently achievable, using the print device as a 'back door' onto the organisation's trusted network.

[1]KYOCERA/iGov Survey 2017 "Print & MFD Management Solutions in the Public Sector.

Crucial to the consideration of any print security plan is an understanding of the present security and compliance capabilities available from market-leading products.

Print security capabilities.

Crucial to the consideration of any print security plan is an understanding of the present security and compliance capabilities available from market-leading products. This is in addition to standard security practices such as deploying the devices behind enterprise firewalls, routine updating of passwords, and bringing print-related activities into the scope of broader employee acceptable IT usage policies.

Harnessing the following properties, and enforcing their use, are key to the development and implementation of any print security plan:

Interface blocking/network configuration

Ensure that data theft via USB is prevented by utilising port blocking. Ideally, the device should be capable of enabling blocking according to usage, so that legitimate use of the USB port (e.g. to support a keyboard or IC card reader) can still be supported. Look for capabilities that allow USB functions to be disabled at device, host and storage levels.

Another exploit to guard against is attack via an unused port or transmission protocol. Ensure you disable/close unused protocols and ports. If your device is capable of sending faxes then this could also be a critical vulnerability. Either disable this feature or (if you use faxes) employ settings such as prohibiting broadcast transmissions and redialling, and set sending limits.

You can also configure your devices to only communicate with terminals using known IP addresses, and within network environments where all terminals are certified to the IEEE 802.1x standard for network connections, which supports a range of cryptographic methods.

Encryption & secure transmission

Encryption protocols such as SSL/TLS (Secure Sockets Layer/Transport Layer Security) and/or IPSec should be supported as these protect data transmissions across the network connection from leakage and falsification. The latest devices should also support SNMPv3 (the most advanced version of the Simple Network Management Protocol) which — when enabled — encrypts its transmission.

Strong encryption algorithms should also be included as features on hard-disk drives and solid-state drives (HDD/SSD) to protect them from exploitation. Other related features include the ability to auto-delete temporarily stored image data from scan and copy jobs once the data has been processed, and the use of encrypted PDFs that require recipients to use a password to view. Both mitigate the risk of unauthorised data access.

User authentication

There are two approaches to authenticating registered users' access to print devices: local authentication and network authentication. Both can be used concurrently. Local authentication pertains to the user information stored on the MFP, while network authentication uses certification stored on Active Directory, Kerberos and/or other authentication servers. Both approaches can utilise PIN codes and card reader technology, and two-factor authentication based on a card/password combination. These measures prevent unauthorised access to data and enable activity monitoring and logging.

Access control

Print devices are shipped with default administrator passwords and these should be changed immediately. This is critical to preventing security risk such as false or malicious changes to user registration information, network settings, address books and/or text data, as well as unauthorised access to the device. This step should also be taken for any centralised and/or web-based management portal overseeing the entire print estate as well as for individual devices.

'Brute-force' attacks (whereby different username/passwords are continuously attempted until access is gained) can be mitigated by employing an Account Lockout feature, where users are suspended from access after a certain number of login failures, and for a fixed duration, both set by the administrator. This can be applied both at the network and local authentication level.

Another useful feature for access control is the 'Document Box', which is ideal for storing sensitive scanned or printed data.


KYOCERA
TASKalfa 6053ci
Plain A4
Plain A3
Thick A4
Custom BS
Thick A4

Setting access permissions by user or user role helps prevent information leakage by insider attack and/or human error.

Usage control

Setting access permissions by user or user role helps prevent information leakage by insider attack and/or human error. Utilisation limits for copying, printing and scanning data, faxing, and storage are some of the basic parameters available on modern systems.

Take advantage of 'Private Print' features that enable the release of stored jobs only when a PIN code is manually entered on the MFP operation panel. This helps meet compliance for prohibited removal of sensitive printed information or incidental glances at printed pages.

Administrators should also be able to control the other functions available on the device operation panel, depending on the user profile. Panel Lock settings are typically set on a tiered basis, with the default being to limit all system functions. Other tiers would allow access to (for example) network, printer and paper settings.

The ability to set reference authority for editing address books and viewing job status/history should be exercised so that these rights are not unwittingly granted to all users. Consider setting these to administrator level and/or the owner of the specific job.

Document stamping

Printers produce paper documents that often contain sensitive information that malicious persons may seek to copy illegally. By using a custom notification stamp on all printed pages, you can ensure that the publisher source can be traced, even after multiple generations of copies. The stamp may also deter the creation of illegal copies.

Auditing & logging

Preventing unauthorised use or leakage of data may not always be possible, so when issues do occur it is vitally important to have an audit trail of user activity and job history to piece together what happened. This intelligence may also be crucial in a successful and speedy cyber incident response.

Administrators should set up an auditing and logging regime that tracks jobs, logins, device activity and security-related values and errors.

Secure disposal

The final stage of a device's usable life is a potential security blindspot. The device itself should include functions that assist in the shutdown and sanitisation process, overwriting user information with meaningless information to erase it completely, and rendering the device disabled from further use. This should occur before the device is sent for disposal.

Ensure that any plan you put in place is cognisant of future business objectives, digital initiatives and other planned changes within the organisation — particularly those that impact the use of print assets.

Developing your plan.

Any successful print security plan must be purpose-designed for the unique requirements of the organisation in question. As such, the following preliminary steps are essential:

Step 1: Needs analysis

Cybersecurity is a critical board-level consideration for all organisations. Where possible, organisations should include print security considerations as part of their wider risk assessment activities. It may also be pertinent to consult existing information security policies to ensure that protections in place to secure laptops, PCs, databases, etc. are also employed to cover all IP endpoints including print devices.

Consider:
- Developing a Risk Register for Print Assets.
- The requirements for general and industry specific regulatory compliance.
- Impact on organisation-wide cyber incident reporting and response.

Step 2: Workflow mapping

Set out the business workflows that relate to copying, scanning and printing documents within your organisation and identify potential security risks. This exercise may benefit from external consultancy support from a qualified third party, both to provide objectivity and expert insight. This may even produce opportunities to change processes to make them more efficient and/or environmentally sustainable.

Consider:
- Conducting staff interviews to get the most accurate picture of 'real' processes.
- Using the findings to inform common user profiles (e.g. by role, department, etc.).
- Using this as a benchmark to evaluate against in future.

Step 3: Current state of infrastructure

Audit the existing fleet as well as the policies currently employed for data protection and security. Identify what security capabilities are present, which can be added and which can only be achieved through a replacement programme. Examine the current security measures on the enterprise network, and how print devices are configured. Again, all this would ideally be conducted in the form of independent third-party audit both for the reasons listed above, and to add sufficient resources to complete the assessment within a compressed timescale and without missing anything.

Consider:
- Benchmarking the present status against market-leading security capabilities.
- Accelerating replacement schedules for devices approaching end-of-life.
- Collating more asset data (e.g. capacity, energy efficiency) to support other aims.

Step 4: Future user requirements

Ensure that any plan you put in place is cognisant of future business objectives, digital initiatives and other planned changes within the organisation — particularly those that impact the use of print assets. Another aspect is future working practices that your organisation may not fully support, such as flexible and mobile working for employees, and widening the use of IT resources for contractors and office visitors. Where these future requirements can be satisfied by the implementation of new technologies, it is critical that these are only pursued under the auspices of a print security strategy.

Consider:
- Qualifying and quantifying the gap between present and future states.
- Consulting best practice examples of organisations in your sector.
- Being ambitious in what you ultimately want to achieve.

The items described above — together with the known capabilities highlighted in the previous section — will inform the Print Security Strategy, its aims and your desired future state of infrastructure and protections.

The print security strategy should:

Understand the need for change in the context of the current environment

- Identify why additional security measures are necessary and how they mitigate risk
- Get leadership agreement on objectives

Articulate your vision

- Describe, in plain language, the desired end state that your improved approach to print security aims to realise
- What material difference will this make to the organisation and its stakeholders?

Develop a roadmap

- Complete a gap analysis of current versus future, desired state
- Convert into a time-bound and budgeted investment of time and resources to implement deliverables (e.g. both functionality and policy)

Monitor the journey and evaluate success

- Establish KPIs and report regularly

Adapt to change

- Be prepared to accommodate further measures in light of new threats and to capitalise on emerging security capabilities

Critical success factors for implementation.

Kyocera works with leading organisations around the world and in every sector to implement document and print solutions that are secure, efficient and sustainable. These projects benefit from the industry-leading data security capabilities of Kyocera's products as well as a wealth of experience addressing changing security and compliance demands in the face of increasingly sophisticated cyber threats.

Based on this unique perspective, here are some of the common critical success factors for the implementation of print security strategies:

Gain sponsorship from the board

Cybersecurity relies upon policies and technologies, but it can be seriously undermined by the wrong organisational attitude. A strong culture of data integrity and governance should be set at the highest levels, with business leaders setting the tone for identifying and responding to cyber risks. Strategic print security projects that happen in isolation from senior-level ownership and accountability are more prone to delays and other avoidable shortcomings.

Bring users with you from the start

The new policies and features you plan to introduce are likely to save time and reduce manual tasks, as well as to improve security. But some employees will find change uncomfortable. The key is to focus on the benefits, and work to reduce the impact upon working practices to maximise flexibility. By enthusing staff from the outset, you maximise the chances of swift and successful adoption of your newly prescribed practices. This is critical to ensuring that users do not attempt to navigate or subvert new processes with 'workarounds' that bypass security controls and leave data vulnerable to theft, damage or accidental loss. Cyber threat awareness training for all employees is another important consideration to ensure that everyone is aware of their responsibilities and the potential impact of failing to follow policies.

Capitalise on a wider digital transformation

Running the rule over your entire print estate and related document processes is essential for developing a good security plan, but don't underestimate the value of 'killing two (or three) birds with one stone' by applying the same discovery exercise to other IT initiatives. For example, increasing numbers of organisations are proactively seeking to maximise environmental sustainability through a paperless or paper-light digital transformation, and understanding the full extent of their print estate is a key prerequisite. It makes logical sense, therefore, to address data security imperatives at the same time. Whether it's sustainability, efficiency or cost reduction, running IT initiatives in parallel can have knock-on implications for print security, and vice versa. Moving to more digitised document processes — for instance — can enable better data governance, but only if the correct security controls are applied.

Try before you buy

Best practice is to commit to a proof of concept exercise, including trials in a live environment with real users, once you have settled on a roadmap of capabilities and processes. There is no substitute for road-testing as this can often be the catalyst for questions and possibilities that were not previously considered. Another top tip is to explore case examples of live deployments; preferably in your industry sector or size of organisation. Manufacturers and technology partners should be able to facilitate introductions, and these can be extremely useful for seeing different secure working practices and document processes in action.

Phase deployments

There is nothing to fear from executing a well-planned, well-resourced, organisation-wide print security strategy in one implementation phase. However, unless there are compelling reasons for this, a preferred approach would be to stagger the implementation in multiple waves. A phased approach allows you to concentrate your available resources both on implementation day on for any subsequent period of 'hyper-care' internal help desk support. Phases may be logically organised by location (if there are multiple offices), department or user profile.

Stress test your solution

Measure the success of your print security strategy with a testing regime designed to simulate common threat vectors such as unauthorised user access, USB data download and brute force attack. Reputable independent auditors and security testers can be employed to conduct 'penetration testing' to highlight any remaining weak spots and recommend remediation action. Any security testing regime should also take account of 'social engineering' techniques, using role-play to emulate the efforts of malicious actors to obtain passwords and illegally gain access to printed or stored data.

Conclusion.

Many organisations may be tempted to believe that they will somehow remain unaffected by cyber attacks that exploit insecure print devices, or that the attacks that may befall them will have limited impact.

This is a dangerous and misguided view that simply does not stack up to reality. There is no 'security through obscurity', and cyber attackers are well aware that uncontrolled and poorly configured print assets typically represent the easiest entry points onto a target network.

If the willingness is there to pursue a solution, the only remaining challenge is to develop and implement a strategic response. By taking account of the market-leading print security capabilities from manufacturers like Kyocera, and following the practical advice contained in this guide, organisations can bring their print assets under the control of robust security and compliance policy, and look forward to the benefits of a technology environment that benefits its users and is ready for anything.

Kyocera Document Solutions has championed innovative technology for more than 60 years. We enable our customers to turn information into knowledge, excel at learning and surpass others.

With professional expertise and a culture of empathetic partnership, we help organisations put knowledge to work to drive change.

KYOCERA Document Solutions (U.K.) Limited
Eldon Court
75-77 London Road
Reading
Berkshire RG1 5BS
Tel: 01189 311500
Fax: 0118 931 1108
e: info@duk.kyocera.com

KYOCERA

kyoceradocumentsolutions.co.uk