Sneaky data can be the most lethal to any corporate entity – the data that hides in the dark corners of most companies and goes largely unnoticed – until it is found by a bad actor.

Companies now operate in an environment where it is essential to track all places sensitive data (such as personally identifiable information, health information, and credit card data) is transmitted and stored. Main information technology servers, backup systems, local hard drives, portable drives, mobile devices, and email systems are all obvious data homes that require constant attention. But data stored on copiers, facsimile machines, and other mechanical devices does not always come to mind when inventorying and establishing solid data security, compliance, retention, and destruction programs.

Copiers store data when scanning, printing, faxing, etc. and are equipped with smart technology. As such, organizations must treat copiers as other smart technology.

The following is a list of best practices for managing smart copiers/equipment:

Include copiers in your equipment inventory risk assessment, risk management plan, and retention/destruction plans.

Various U.S., state, and foreign laws require that sensitive data be data mapped, secured, and appropriately retained/destroyed. Because smart copiers have drives/memory banks, the use of these devices should be governed by your organization's information security policies. It is also prudent to ensure that copying equipment is managed by the same information technology team that secures data on your company's laptops, smart phones/devices, printers, and other equipment for consistency of approach. The National Institute of Standards and Technology (NIST) has published guidance on standards for securing smart equipment. See NISTIR 8023, Risk Management for Replication Devices. The NIST publication includes a recommended risk assessment worksheet that organizations can use to develop a risk management plan. See NISTIR 8023, p. 30.

The following are example questions from the NIST publication that organizations should address before deploying smart equipment:

- Who will use the device and where will it be located?
- Will the device be connected to a network?
- What is the impact level (i.e., low, moderate, or high) of the information to be processed, stored, and/or transmitted by the device?
- What kinds of capabilities (e.g., high-capacity, network connection, ability to handle special materials) are needed for the device to perform its intended functions?
Will the device be purchased or leased?

What security controls are needed to protect the confidentiality, integrity, and availability of both the device and the information to be processed, stored, and/or transmitted by the device at the appropriate impact level?

What device functionality is needed to support security requirements and provide security at the appropriate impact level?²

Think about security while negotiating leased copy equipment.

Organizations need to know in the contracting phase how a copy vendor will secure, service, and dispose of a copier during and at the end of its life cycle. This will help ensure that your organization obtains favorable contract terms from the leasing company on compliance issues (including training of service staff) and the proper disposal of the hard drive of the equipment. For example, some lease agreements allow for a company to purchase title to the hard drive of the equipment. This may allow your organization to have the hard drive returned to you after your lease expires. Another potential option is for overwriting the data on the hard drive to make the data inaccessible.

The key is to ensure your organization is able to control the destruction of the memory on the hard drive at the end of the lease agreement. Be sure to negotiate the process for wiping the hard drive on the front end and using a skilled professional to handle the destruction/return of data at the end of the lease term. Termination should always be followed by a certificate of return/destroyc that confirms data was timely returned/removed/destroyed in compliance with applicable law and contract terms. Leased copiers should be completely wiped of all residual data before being transferred to the next lessor.

The NIST guidance also recommends that organizations consider procuring equipment with the following security features:

- Editable configuration settings;
- Image overwrite capability;
- Physical protection capability (e.g., ability to be bolted to the floor or secured with a chain and padlock);
- Physical protection for nonvolatile storage media (e.g., requires a lock to access the hard drive);
- Ability to maintain the RD by internal staff and/or maintenance support throughout its expected life span (including software patches, replacement parts, etc.);
- Ability to encrypt information while in transmission or storage (including passwords, configuration settings, and user files);
- Activity monitoring with alerts/triggers (e.g., automatically block suspicious activity);
- Audit record (event logging) capability;
- Authentication capabilities (e.g., password/pin, smart card, proximity badge);
- Access control levels/roles (e.g., administrative/privileged access, user access);
- Ability to configure network/port settings;
- Tamper evident solutions (e.g., anti-lift ink, copy-void pantograph); and
- Automatic safety shutdown (e.g., when overheating).³

Utilize the equipment's security features.

Copiers often come with default settings for administrative rights and security – which should be immediately changed to enhance security before going live. Copiers should be secured with unique access
credentials utilizing multi-factor authentication, and many copiers allow for secure overwriting of the entire hard drive. Use that feature to overwrite the hard drive frequently.

It is also important to remember that a smart copier can provide a portal for an outside cyber-attack. Be sure that all digital copiers connected to your network are securely integrated and protected against outside intrusions and attacks.

Also consider requiring a password, card swipe, biometric information, or other authentication when physically accessing the device. Creating rules to manage print jobs is also a valuable security feature. This allows your organization to restrict access to certain printers and to provide audit trails for investigations in the event of a security incident.

Other suggestions from NIST include:

- Actively communicate with the original equipment manufacturer as necessary to calibrate and configure the device;
- Isolate the device from other systems until it is calibrated and securely configured;
- Place a warning sticker on the device to inform/remind users about the nonvolatile storage;
- Review user accounts and privileges;
- Limit administrative/privileged access to a primary and secondary administrator;
- Restrict users and service technicians from being able to change the configuration settings;
- Restrict/disable remote access (e.g., by vendor/service technicians); and
- Disable any call-home features (e.g., do not allow monitoring of usage by the manufacturer).  

Additional resource:


2 A complete set of questions is included in the NIST standard. See NISTIR 8023, p. 6.

3 See NISTIR 8023, pp.7-8.

4 See NISTIR 8023, pp. 8-9.