# ITL BULLETIN FOR APRIL 2015

## IS YOUR REPLICATION DEVICE MAKING AN EXTRA COPY FOR SOMEONE ELSE?

Celia Paulsen, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

### Introduction

A replication device (RD) is any device that reproduces (e.g., copies, prints, scans) documents, images, or objects from an electronic or physical source. Historically, the capabilities of RDs were limited, and the security of information processed by RDs was not generally a consideration for most organizations. For example, devices did not save scanned or printed information, and they weren't connected to the Internet, but were stand-alone devices or connected directly to a computer by a cable.

Today, however, RDs are often connected to organizational networks, have central processing units that run common commercial operating systems, are combined with several additional functions such as email or telephone capabilities, and they may store a variety of information internally on nonvolatile storage media. As a result of this increasing functionality and connectivity, RDs may be vulnerable to a number of threats if the risk is not mitigated using appropriate security procedures and controls.

ITL has released Interagency Report (IR) 8023, Risk Management for Replication Devices, which provides organizations with guidance on protecting the confidentiality, integrity, and availability of information processed, stored, or transmitted on RDs. This report also identifies activities to help organizations manage risk associated with such devices.

### Threats and Vulnerabilities

NISTIR 8023 emphasizes that the potential impact of RD compromise depends on the information the device handles or processes, and on the capabilities of the device. For example, while confidentiality of information processed may be a primary concern with regard to a device used to copy personally identifiable information, integrity of the device may be of greater concern for a three-dimensional (3D) printer which uses laser sintering of metal powders to manufacture replacement parts for a boat.

The report identifies threats and vulnerabilities related to RDs. Identified threats and vulnerabilities fall into three categories: general, those related to network connectivity, and those related to nonvolatile storage media.

Some of the threats and vulnerabilities described include:

- Account/password weaknesses: Many devices are provided to the consumer with easily discernible or default administration accounts and configuration passwords.
- Unencrypted information: Unless encrypted, data transmitted or stored, including passwords, configuration settings, and data from stored jobs, is vulnerable to interception or modification.
- Alteration/corruption of data: If passwords or configurations are changed, users could be unable to access or use the RD, documents or objects could be printed incorrectly, and there could be damage to the device.
- Outdated and/or unpatched software and firmware: Many devices run an embedded operating system, making them subject to the same threats as any other computer running those operating systems. Also, some devices may have software or firmware that is not updatable or no longer supported by the manufacturer, which may leave unpatched security issues.
- Open ports/protocols: Open ports and protocols allow data to flow to and from a device. Through open ports, attackers may gain undetected access to a device, and data tampering or denial of service can result.

**Risk Management**

The report emphasizes the importance of considering information security in each stage of the RD's system development life cycle. To help organizations manage risks associated with RDs, NISTIR 8023 provides guidance on identifying and implementing appropriate risk management strategies throughout the system life cycle. The guidance is mapped to related controls in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, where appropriate.

In addition, NISTIR 8023 provides a sample information security risk assessment of RDs. This sample assessment includes a risk assessment table containing risk-related questions which are tied to a risk score. A security risk assessment flow chart is provided as another view of the sample security assessment. The total calculated risk score allows an organization to define three levels of risk (High, Moderate, and Low) and appropriate cybersecurity actions. Organizations may use the risk assessment to identify problem areas, define appropriate mitigating actions, or justify accepting the risks.

The report encourages organizations to add, change, or remove questions and assumptions, recalibrate the risk scores, and make any other revisions needed to adjust the guidance to specific organizational security and operations requirements.

**Conclusion**

The risks associated with using RDs continually evolve. As technology, the operational environment, and an organization changes, the threats, vulnerabilities, likelihood, and potential impact of an event may also change. NISTIR 8023, *Risk Management for Replication Devices,* encourages organizations to assess risk when acquiring a RD and on a regular basis throughout the entire system life cycle to ensure the implementation of appropriate countermeasures or mitigation strategies.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.