Duff on Hospitality Law

Don't Forget Copiers, Scanners and Fax Machines in Your Data Security Program

03.13.15 01.07.26

How secure is the data on your office copier? Today's post from Benjamin Lambiotte, technology and data privacy attorney in Garvey Schubert Barer's D.C. office, outlines the data security risks associated with office machines, as well as the warning signs and steps that you can take to reduce those risks. Thank you, Ben! – Greg

Current generation multifunction printer/scanner/copier devices are convenient, inexpensive, and very popular. Often overlooked is the fact that most modern printers, copiers, and scanners have many of the same attributes of computers, and are just as vulnerable to the same kind of cyber exploits and attacks as computers. A truly comprehensive data security and privacy risk management approach requires that these commonplace devices be viewed as an integral part of an enterprise's IT systems, and that device-specific measures be taken to secure them. The National Institute of Standards and Technology ("NIST") last month published a report on risk management practices for "replication devices." The NIST report identifies risks associated with such devices, and provides guidance on protecting the confidentiality and integrity of information processed, stored, or transmitted on them.

Risks

Threats include:

- Default administration/configuration passwords: Many devices have default passwords which can be easily obtained and used to access stored data, or to control the device.
- Data capture: Unless encrypted, data transmitted or stored, including passwords, configuration settings, and data from stored jobs, is vulnerable to interception or modification.
- Spam: Unless properly configured and without proper access control, many devices will process any job submitted, which could waste paper, toner, and ink, and tie up the device.
- Alteration/corruption of data: If passwords or configurations are changed, denials of service for authorized purposes or potential damage to the device could result.
- Outdated and/or unpatched operating systems 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, older devices may have embedded versions of operating systems no longer supported by the manufacturer, which may leave "unpatched" security issues.

- Open ports/protocols: For devices that can connect to local networks or the Internet via wireless or ports, open ports and protocols allow data to flow to and from a device. Through open ports, attackers may gain undetected access, and data tampering, unauthorized access, and denial of service can result.

Warning Signs

The Report identified several signs indicating that the security of such a device may be compromised:

- Display malfunctions or shows incorrect information;
- Materials (ink, paper, or other supplies) run out faster than usual;
- Increased number of failed or timed-out jobs;
- Unexplained/unauthorized changes in configuration settings;
- Device completes processes slower than expected;
- Device uses more network time/bandwidth than usual;
- Time stamps do not align or make logical sense;
- Communications with unknown IP or email addresses increase; and
- Markings indicating tampering around key areas of the device (e.g., hard drive or SSD compartment, display area).

Countermeasures

An Appendix to the Report provides a very useful device risk assessment template and checklist. It gives practical guidance on best security practices, across the entire lifecycle of the device. Examples of some countermeasures include:

- At acquisition, or in third party supply and support contracts, ensure that the device meets common data security standards, is capable of operating in a secure mode, and that the OS is actively supported by the OEM;
- At deployment, change vendor default passwords, and configure the device to operate in a secure mode;
- During operation, control device access through PINS and passwords, control physical access to the device itself and its components, such as the SSD or hard drive, and track usage, ensure that stored and transmitted data are encrypted, and timely implement OEM security "patches" and fixes;
- During operation, control network access using standard organization practices, close unused open ports and protocols, disable wireless identifier broadcasting, and configure the device to prevent communications to and from unknown and unwanted addresses (blacklist/whitelist); and
- When taking the device out of service, change all passwords and PINS to vendor defaults, and remove or sanitize all hard drives and SSDs on which data may be stored.

The NIST report is available here.

If you have any questions, or for more information on data security, please feel free to contact me or Ben, directly.

Foster Garvey

Posted in Data Privacy, Technology

Tagged as data security, National Institute of Standards and Technology (NIST)