

December 5, 2011

Dear Kyocera Mita Canada Dealers:

MSNBC recently reported a study that identified the potential unauthorized access of a company or small business network through a specific brand of connected laser printer.

Kyocera Mita is serious about its commitment to security in all of its products. Although Kyocera printers were not mentioned in this report or study, we understand that your customers may perceive this as a potential threat with Kyocera devices. Kyocera ECOSYS printers come standard with an array of security features that can help answer your customers' questions regarding this report on MSNBC.

When seeking a higher level of security, these security features will help to prevent unauthorized access to the network through the device. These standard features include, but are not limited to:

- **Remote Firmware Upgrades:** Companies looking to upgrade the firmware on a fleet of Kyocera devices need to contact an authorized Kyocera servicing dealer. Firmware from Kyocera is not made publically available and can only be installed or upgraded remotely under the following conditions: The Kyocera servicing dealer has access to the most recent remote firmware packet; Kyocera's proprietary monitoring and tracking utility must be running on the customer's network, and access must be granted by the customer to their network. Only at this point would an authorized Kyocera servicing dealer be able to upgrade a customer's firmware.
- **IP Filtering:** In an Enterprise environment or any location using a Print Server setting, an IP Filter will allow customers to limit network communication to just the authorized Print Server.
- **Set Allowed IP Ranges:** Limit communication to the connected device to only PCs on an internal network and selected IP range. Companies can also enter a number of individual addresses instead of a range, if desired.
- **Block Specific Printer Ports:** Companies can limit access to the device allowing selected supported protocol ports to accept data on allowed IP Addresses. Kyocera devices support LPD, FTP, IPP, HTTP, Raw, SNMP, IPPS, and HTTPS. Kyocera also supports SSL, IPsec, and other secure communication protocols.

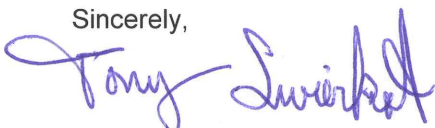
The MSNBC report also mentioned the increased risk of fire through access caused by unauthorized firmware. Kyocera ECOSYS printers are designed and tested to meet the strict testing requirements set by UL and CSA.

A requirement of these safety certifications is a 'Thermocouple' that will prevent the risk of overheating and/or fire by shutting down power to the heating element, which can only be restored by an authorized Kyocera technician. This is built into the hardware and cannot be modified or altered through firmware.

Kyocera recommends that any network with Internet access should have a firewall in place to protect all the connected printers, MFPs and PCs, preventing external unauthorized access of a company's devices. Following good network security practices is a key component to protecting your infrastructure.

If you have any questions or comments regarding the security of Kyocera devices, please feel free to contact me directly.

Sincerely,



Tony Swierkot
Marketing Manager
Kyocera Mita Canada, Ltd.