



Secure Print and Data Loss Prevention: Minimizing the threats of internal data leakage

Today's security threats are numerous and widespread. Whether it is the constant barrage of external attacks or internal malicious behavior by employees, organizations around the world are struggling to minimize data leakage to the public domain.

While many organizations spend incredible amounts of time, energy and resources to fend off external attacks, only a small portion spend enough of those resources on establishing a security policy that addresses the most inherent risks associated with the removal or transfer of sensitive information. Gartner analyst Richard Hunter indicates that, "more than 70 percent of unauthorized access to information systems is committed by employees, as are more than 95 percent of intrusions that result in significant financial losses". Most of these data breaches are not caused by malicious behavior, but rather by employees unaware of the confidential nature of the data, a lack of an established policy or the lack of education of said policy.

Some organizations have policies in place that govern the use and misuse of company computers and laptops. Others address the use of the internet, instant messaging, email and the access of confidential files. One major omission on almost all security policies is the use of printers, scanners, copiers or all-in-one MFP devices. Because these devices many times are endpoints within an organization's network, they are susceptible to misuse. As the Multifunction Printer (MFP) has developed, additional features, such as scan-to-email, have become prevalent and standard operating procedure for many employees. The result is a powerful device able to print or copy documents, scan images and directly email to any electronic destination. At the same time, in many cases they are unmonitored and therefore high security risks for an organization.

One way to minimize these risks is to establish use policies with Print Management Solutions. These software packages allow organizations to rectify this scenario by establishing rules governing the use of these MFP devices, preventing employees from using certain functions of the device. A key aspect of this solution is the authentication of users at the MFP. By identifying the user whenever the device is accessed, certain rights and privileges can be granted or denied based on department, hierarchy and position. When an employee prints to a device, the print job is delivered to a queue where the document can be checked against pre-set rules. If the employee has authority to print this document, then after the employee presents their company identification card to the MFP, the document will be released from the print server and delivered to the printer.

This is just one example of the many ways Print Management Solutions and Secure Print Authentication can minimize the risk of internal data leakage. HID has partnered with the best of breed Print Management vendors as well as all the major manufacturers of Multifunction Printers to work with organizations to eliminate this typically unaddressed gap in their Data Loss Prevention policy.