Security :: Multifunction Copier/Printer Devices

Multi-Function Devices (MFDs) are much more powerful than their photocopier-like appearance implies. Their multi-functionality (fax, scan, copy, print) means that their internal hard drives store a great deal of data and, because the devices are connected to both the Internet and the network, that data is vulnerable without appropriate security measures in place. Read more about MFD security [1].

A Multi-Function Device (MFD) is a device that provides centralized printing, scanning, copying, and faxing functionality; HSU has a number of these devices in offices around campus. MFDs are both network- and Internet-connected, so in many ways they function in a similar fashion to a computer. For this reason, and because they are multipurpose devices, it's vital that they are appropriately configured and managed to protect the information that passes through them.

It's easy to forget that these devices are much more powerful than the photocopier they most closely resemble, and their very multi-functionality creates a number of potential security risks. Without appropriate security configuration on the device, information may be inadvertently moved across the network or stored in plain text--which offers no protection against hacking and other unauthorized access. If Level 1 [2] or Level 2 [3] data passes through the device, the way that data is handled must comply with the same campus security standards as are applicable to computers that handle protected data. These standards are based on FERPA [4], HIPAA, CSU Information Security Standards [5], and HSU Procedures [6].

Responsibility

Any individual who handles sensitive data is required to understand and comply with requirements for protecting it. This is covered in the confidentiality agreement you signed when you first became associated with Humboldt State University.

Additionally, Work Area Administrators (department heads) are required to:

- Understand the security risks inherent in the use of MFDs
- Train users in the appropriate use of MFDs
- Ensure that appropriate security procedures for handling sensitive data are followed
- Promptly report any suspected security incidents [7].

Potential Security Risks for MFDs

- Printing, scanning, copying, and faxing functions, without proper security configuration, may result in the transmission or storage on the hard drive of sensitive information in unencrypted (plain text) form. Processing Level 1 or Level 2 data on an unsecured MFD can leave it vulnerable to hacking and identify theft.
- An MFD has many functions that allow it to be easily used in various business environments. If these services are not secured, they can be exploited by hackers, launch a denial-of-service attack, install malware [8], or gain unauthorized access to the data on the MFD.
- When the MFD is serviced, traded, transferred or retired, the internal hard drive must be wiped, removed or destroyed following the HSU Procedure for Transfer and Disposal of Media [9]. If documents and data remain on the MFD, they can fall into the wrong hands, which could have serious legal repercussions for the University.

Minimizing the Risk

- Consider the availability of security options such as encryption [10] or hard drive overwriting before purchasing
- Any areas that process Level 1 or Level 2 data should purchase an MFD with encryption capability
- Devices configured for Level 1 or Level 2 data must conform to CSU and HSU Security Standards and Procedures.
- Area Administrators should use the Multi-Function Device Checklist for Area Administrators [11].
- Area Administrators should post a sign above each MFD that indicates: this MFD is approved for Level 1 or Level 2 data [12] or this MFD is not approved for processing Level 1 or Level 2 [13] data.
- For MFDs that process Level 1 or Level 2 data, the Desktop Support Specialist should complete the MFD Hardening Checklist [14] and have it be verified by the Area Administrator.

Related Topics

Tools & Resources [15], Security [16]

Source URL: http://www2.humboldt.edu/its/security-multifunction

Links:
[1] http://www.humboldt.edu/its/security-multifunction
[2] http://www2.humboldt.edu/its/glossary/5#term224
[3] http://www2.humboldt.edu/its/glossary/5#term293
[4] http://www2.humboldt.edu/its/glossary/5#term298
[5] http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf
[6] https://www.humboldt.edu/its/sites/its/files/docs/lvl1-Sec-Standards-approved-6-8-10.pdf
[7] http://www.humboldt.edu/its/security-incidentresponse
[8] http://www2.humboldt.edu/its/glossary/5#term200
[9] https://www3.humboldt.edu/iso/ITC016-media-destruc-proc-appr-rev%209-19-12.pdf
[10] http://www2.humboldt.edu/its/glossary/5#term239
[11] https://www3.humboldt.edu/iso/MFDChecklist-Area-Administrators-3-15-13.pdf
[12] https://www3.humboldt.edu/iso/OK-MFD-sign.pdf
[13] https://www3.humboldt.edu/iso/NOT-OK-device_signage.pdf
[14] https://www3.humboldt.edu/iso/HSU-MFD-Hardening-Checklists-ITCs.pdf
[15] http://www2.humboldt.edu/its/category/quicklinks/tools-resources
[16] http://www2.humboldt.edu/its/category/quicklinks/security