

Establishing a Secure Document Production Environment

SITUATION ANALYSIS

Without a doubt, security is of the utmost importance in today's business environment. While many companies have taken extensive measures to protect corporate network infrastructures, one of the most overlooked areas in establishing a security strategy is the document production environment. According to the Association of Certified Fraud Examiners, U.S. companies lose more than \$600 billion to fraud each year, with counterfeiting and document fraud making up more than two-thirds of that amount. The reality is that your company's multifunction products (MFPs) that copy, print, fax, scan, and electronically store and transfer your documents are an integral component of the corporate security strategy — data communication throughout the entire corporate network must be securely stored, transmitted, and received.

Multifunction devices have evolved in recent years to support numerous functions integrated within the corporate network infrastructure. Features such as document storage and scan-to-e-mail make document production equipment as much a part of the network as computer systems. Because of this increased network functionality, security measures must be taken to ensure data integrity and accountability going to and from the device. This includes data communication within the corporate network, as well as outside the firewall. Furthermore, for companies that must comply with current government regulations, it is mission critical that they have adequate security safeguards in place to meet or exceed compliance guidelines.

GOVERNMENT REGULATIONS AND STANDARDS

New government mandates are requiring companies to tighten data security. It is imperative that companies ensure that their information technology (IT) assets enable them to comply with these new initiatives and protect the integrity of confidential company and customer information. Some of the major regulations that can be addressed with a secure document management strategy include:

- **Health Insurance Portability and Accountability Act (HIPAA)** – One of the most widely recognized regulations, HIPAA is designed to ensure that patient information is treated with the highest level of confidentiality, both within the healthcare organization and when information is transferred between institutions and healthcare professionals. Secure device access, private printing features, and audit trail capabilities can prevent improper device usage and allow only authorized users to receive confidential patient data or documents.
- **Gramm-Leach-Bliley Act (GLBA)** – GLBA was written for financial institutions, ensuring that consumers are aware of how their personal financial information is being used and shared. The act's Financial Privacy Rule and Safeguards Rule govern the disclosure of private financial information and require all financial institutions to design and

maintain systems to support the protection of customer information. Financial services companies must protect sensitive customer information from security threats and maintain data integrity. Some of the key features for compliance available on the industry's most advanced MFPs include user authentication, hard drive data overwrite and data encryption.

- **Family Education Rights and Privacy Act (FERPA)** – FERPA is a federal law that protects the privacy of student education records, requiring a heightened level of security for educational institutions complying with the U.S. Department of Education. Password printing, controlled device access, data encryption and deletion of stored data ensure that sensitive information is not accessible from the multifunction device. These features also aid educational institutions in limiting the number of users that can access and retrieve student records, further enhancing privacy and security.
- **Sarbanes-Oxley Act (SOX)** – Following recent high profile corporate scandals, SOX was passed to protect investors by improving the accuracy of corporate financial disclosures. SOX also introduced stringent rules with the objective of changing financial practices and corporate governance regulations. Data security safeguards required for SOX compliance and available on many MFPs include restricting access to information, tracking data, securing output, overwriting data and protecting data integrity.
- **Common Criteria Evaluation and Validation Scheme (CCEVS)** – Established by the National Information Assurance Partnership (NIAP), the Common Criteria program evaluates IT products for conformance to the International Common Criteria for Information Technology Security Evaluation. The program recognizes and validates security solutions based upon an internationally accepted methodology. Companies that are purchasing new document production equipment should seek devices that offer security features that have been either Common Criteria certified, or are currently undergoing certification.
- **The Department of Defense (DoD)** – Operating directly under the President of the United States of America, the DoD formulates national security and defense policies. The Department of Defense Manual outlines rigid policies and standards in the interest of protecting the security of the United States. Features such as overwriting data comply with the DoD standard of clearing and sanitizing a hard disk drive containing classified information.

DATA SECURITY TECHNOLOGY FOR MFP DEVICES

To achieve compliance with the regulations mentioned above, as well as to protect company and customer data, companies must take measures to ensure that their document production equipment is secure. Whenever pages are printed, copied, scanned or faxed, the MFP device may retain data in its internal memory. Without proper security measures in place, this data can be retrieved

by unauthorized personnel, both internally and externally. Additionally, unrestricted access to the device can lead to security breaches, resulting in manipulation, deletion and theft of sensitive data such as proprietary information or intellectual property.

Document output equipment and solutions are available with a wide range of features to achieve a maximum level of security when copying, printing, faxing, scanning or transmitting information. Users should look for an equipment manufacturer that provides security offerings addressing the following four areas:

1. Controlling access to the device and data
2. Data tracking and accountability
3. Protecting sensitive corporate data
4. Securing Communication

Controlling Access – Your First Line of Defense

Companies can control access to their output equipment by limiting which, and how many, users can access the devices, as well as limit which functions can be used. By controlling access, companies can prevent unauthorized users from retrieving data that could potentially be exploited. Access to the multifunction device can be controlled through a number of methods, including the following:

User Codes – Not only do user codes control access, they also provide beneficial data tracking and usage information. User codes require users to enter a code in order to use the MFP device. Codes may be required for all walk-up functions, including copying, scanning and faxing, as well as printing from the desktop. Users are required to input a five-digit code either at the control panel for copy, fax or scan functions, or within the print driver when sending print jobs from a computer. Device administrators are able to easily track and view the volume and type of jobs being produced by each department or user. Additionally, these codes restrict unauthorized users from abusing company resources or gaining access to confidential information.

Network Authentication – Authentication provides an additional means of device control via the network and is ideal for larger scale installations with numerous users. With authentication, users are required to input their network user name and password to gain access to the control panel. Network administrators can control access to the device in the same manner that they control network access from the desktop. If a user is authorized on the corporate network, then he or she can gain access to the MFP. Authentication ensures that only those users who have been authorized can gain access to data stored on the device. In addition, it lets e-mail recipients know the identity of the sender, deterring users from sending prohibited material.

SmartCard Authentication – SmartCard Authentication offers extensive security features designed to eliminate unauthorized operation and reduce costs and downtime. By utilizing a streamlined, single point of entry, it facilitates the user log-in process by requiring a card swipe instead of typing a User Name and Password. With security taking a top priority among many companies, Toshiba is committed to providing solutions that ensure data integrity and accountability going to and from the MFP device. You control who has authorization, thereby maintaining cost efficiency and security.

Private Print – This functionality offers complete control of print output, requiring users to input a password before their document is output from the machine. When users walk up to the device to retrieve their document, their individually selected confidential password must first be entered. The password will then release each selected document sent by the same user. Manufacturers such as Toshiba also offer a batch private print feature to enable users to release all print jobs under the user's print queue. This eliminates the need to re-enter a password for each individual document if the user has sent multiple jobs. Private print is ideal for organizations printing confidential information, and prevents other people from accidentally or intentionally picking up the wrong print job. The private print feature is essential to controlling print data and output at the MFP.

Secure PDF – Much like the private print feature, further control and protection are needed when scanning documents to email and network locations. With Secure PDF, users can assign a password to scanned PDF documents directly from control panel of the MFP. The password allows for various levels of control such as access, printing, editing and copying the content. Furthermore, up to 128 bit encryption can be applied to ensure it is stored safely. Secure PDF is the perfect solution for those wanting to email or store scanned documents without compromising the content.

Usage Limitations – Usage limitations allow the administrator to control and track output at the device. With usage limitations, administrators can limit the number of copies or prints available at an account or a department level. The use of color also is an optional restriction when dealing with a color-capable device. This in turn provides a further level of security to complement the controlled device access, as well as the visibility to track and control costs associated with the device's use.

Strong Passwords – With the advent of password recovery tools that can crack passwords instantaneously, it is recommended that administrators create a strong password. A strong password is one that is at least eight characters, includes a combination of letters, numbers and symbols, and

is easy for the user to remember, but difficult for others to guess. Unauthorized persons will find it difficult to access the administrative and network properties of each device, as well as to gain access to the device's control panel without the proper username and password. For further protection, oftentimes a login limitation of up to three times can be employed. This sequence slows down the ability to crack the password by locking the screen after three failed attempts. Login restrictions can prevent attackers from impersonating users and thereby prevent the loss, exposure, or corruption of sensitive information.

Data Tracking and Accountability – Manage Workflow Both Inside and Outside the Organization

Beyond simply controlling access, companies must ensure that the MFP itself does not present a threat as a result of potential misuse. Many manufacturers offer a variety of features for tracking usage activity, including those listed below.

E-mail Authentication – When conducting business via the Internet or e-mail, it is crucial for the user to know that he or she is corresponding with an authentic addressee. E-mail authentication technology allows organizations to manage e-mails being sent from each MFP. When e-mail authentication is enabled, all scan-to-e-mail users must have a valid e-mail account within the corporate directory. By requiring each user to login to the device and validate their e-mail against the corporation's e-mail directory, users are prohibited from sending anonymous or fraudulent e-mails. The immediate benefit of e-mail authentication is to allow legitimate senders to "prove" their identity and to provide receivers the tracking and accountability to feel comfortable about the information they are receiving. In addition, the administrator can limit e-mail transactions to only those users listed in the corporate address book, preventing company data from being sent outside of the organization.

Remote Administration Utilities – Remote administration utilities, such as Toshiba's Web-based TopAccess program, allow the administrator or user to remotely manage and oversee activities at the device from their desktop. IT managers simply input the IP address of the MFP device into their Internet browser, which then allows them a real-time view of the device status. Other administrative features enable IT managers to set up device settings and network properties directly from the desktop. The advantage of remote administration utilities is that password protection enables only the administrator to modify the device settings, preventing tampering with or potential misuse of the system.

Job Log – The job log feature is a valuable tool for network administrators, dealer service technicians and office administrators, making it effortless to

track data and documents. Print, copy, fax and scan jobs are tracked with detailed information including user, date, time, number of pages, type of paper, and type of job. The job log can then be exported into a standard .csv file for importing into other third-party applications. This data tracking and accountability report provides useful information as to the types of usage at the device, volume, and user.

Lightweight Directory Access Protocol (LDAP) Authentication – LDAP authentication provides a centralized address book of all employees and enables the administrator to establish rules and access rights based on specified user groups. For example, the administrator may prohibit employees employed by the company for less than 90 days from scanning or faxing. With LDAP authentication, the rules set by the administrator will apply to all MFPs on the company network. Another benefit of LDAP authentication is that it ensures that when scanning, the user's name appears on the document. This prevents users from sending malicious or other prohibited material over the corporate network.

Protecting Sensitive Corporate Data – A Deep Cleaning for Your MFP Devices

Most MFPs on the market today offer a standard hard disk drive that provides large storage capacity. In addition to storage, the hard disk drive is used to manage all data flow into and out of the device. As the image data is transmitted or scanned into the device, it is stored temporarily in the hard disk drive until processed. Additional steps are needed in order to completely render all data on an MFP's hard drive completely useless. There are several options to protect the integrity of the hard disk drive and your network data, even in the event of theft of the hard drive or retrieval and misuse of information residing on the drive.

Advanced data protection capabilities include the following:

Hard Drive Encryption – Encryption is the most effective way to achieve data security. Encryption technologies, such as Toshiba's Scrambler Board, feature encryption and decryption of all data being written to the hard disk drive of the device. This includes all copy, print, fax and scanned information processed on the MFP. This encryption technology uses cryptographic algorithms to protect the information stored on the hard drive, with no performance delays for printing, scanning, copying or faxing. Encrypting a file makes the data unrecognizable to other applications and immediately renders the data useless in the event of theft. Residual data also can be completely erased when the encryption device and the hard disk drive are removed from the MFP.

Data Overwrite Kits – Data overwriting ensures that the hard drive is absolutely clear of readable data. It works by overwriting the actual data with random and numerical characters. In addition, the disk is automatically cleared immediately after the device is done using the information after every job, preventing the data from being recovered by unauthorized users. It is recommended that users seek data overwrite technologies that exceed the DoD guidelines of a three-pass standard for secure overwriting, of which all of Toshiba's MFPs achieve when the data overwrite kit is installed.

Encryption technologies and data overwrite kits can be combined for a heightened level of security. The advantage to having both options installed is that information written to the hard drive is rendered useless, while stored information on the hard drive is encrypted. This provides a maximum level of security to ensure that all forms of data are protected.

Securing Communication – Keeping the flow of data safe

As with network computers, MFP devices use several protocols and communication methods when printing or accessing information over the corporate network. To ensure that the highest levels of network protection and secure communication are upheld, Toshiba MFPs employ a wide range of measures to combat potential security threats.

VxWorks Operating System - Toshiba MFPs run on the VxWorks operating system. VxWorks is the most widely adopted real time operating system (RTOS) and is a closed source, proprietary OS. Unlike open source code systems like Linux, VxWorks offers completely proprietary and secure code to facilitate an increased level of security. Furthermore, VxWorks is not susceptible to the viruses that attack Microsoft and Linux operating systems. These security advantages are the foundation of Toshiba MFPs and the basis for why VxWorks is utilized.

IPv6 – IPv6, also referred to as the next generation Internet Protocol, is the latest version of IP. With the introduction of the Internet in the 1990's and its ever increasing use through the years, came the need for a larger pool of available IP addresses, hence the birth of IPv6. IPv6 offers several features to address IP security needs such as:

- Increased address size – the length of the address field from IPv4 to IPv6 has increased from 32 bits to 128 bits. The address structure also provides more levels of hierarchy.
- Built in support for authentication
- Stronger confidentiality

SSL - Secure sockets layer (SSL) is a cryptographic protocol widely used on the Internet to provide secure communications for transfer of personal information during online credit card transactions, order fulfillment, and accessing online accounts. MFP devices employ this common encryption technology to protect all data traveling to and from the MFP. Print jobs sent via the SSL layer are encrypted through symmetric cryptography, ensuring that the print data is secure and will not be used for any purpose other than print output. It prevents the interception of information for malicious purposes or data tampering.

IP Filtering – IP filtering essentially acts like a firewall to protect your internal network from intruders. IP filtering lets you control what IP traffic to allow into and out of your network by filtering data from specified network addresses. MFP devices utilize this mechanism as a means of controlling which computers have access to its network functions

SMB Signing - SMB (server message block) signing is a form of data authentication. During network authentication, once the MFP is authenticated on the server, SMB signing adds a digital signature to the data transferred between MFP and server. The signatures verify that the identity of the server matches the credentials expected by the MFP, and vice versa. By verifying that the data received comes from an authenticated source, the signature ensures the integrity of all communications.

Protocol and Port Control – Toshiba MFPs allow for control of protocols and ports so that security can be tailored to meet your specific needs. When a specific protocol is disabled, the corresponding port is also closed. The following protocols and ports can be disabled:

- HTTP, FTP, LDAP, SMTP, POP3, SNMP, TCP/IP, IPv6, IPX/SPX, AppleTalk, SMB, LPD, IPP

Fax Connection – Toshiba fax devices comply with ITU (International Telecommunications Union) standards. If any of the data received by the fax device does not meet these standards the transmission is rejected. There is no direct connection established between the fax and controller. All communication between the fax and the copier HDD is via a VxWorks interface using proprietary coding. To retrieve the fax image, the controller must interface with the copier HDD via a separate, proprietary coded VxWorks interface.

SUMMARY

While industry sector requirements vary, one thing remains the same – security needs to be applied consistently across your network. The security level of your company’s fleet of document production equipment should be at the same level as the data residing on the company’s computers, or any other networked peripheral. By selecting and implementing appropriate security technologies that are designed to control access, provide data tracking and accountability, and protect sensitive corporate information, companies can improve the security of their network, as well as meet current government regulations.

#

Written by Joseph Contreras
Senior Product Manager
Toshiba America Business Solutions, Inc.
