Encompass Security White Paper

Contents

Prepared by:
Peter Davey
Director of Professional Services
Toshiba America Business Solution
August 15th 2009

Introduction

Introduction.

Businesses are at risk from unsecured MFP and printer devices, weak access controls, unsecured documents and limited employment of secure asset disposition policies. While IT infrastructure, enterprise collaboration and business application security has matured and become a critical facet of information technology, MFP's, printers and documents remain a critical source of vulnerability.

As MFP's in particular become on-ramps to corporate networks and the broader public internet, unsecured, they can be exploited by external threats or misused internally to leak corporate knowledge to competitors and into the public domain.

The regulatory environment has expanded in recent years and legislation often contains provision holding corporations accountable for the security, privacy and retention of documents.

A variety of security vulnerability countermeasures exist for MFP's and printer devices however in order for them to be effective they must be employed holistically and as part of an overall security policy.

Toshiba's Encompass Security Solutions incorporate assessment services, countermeasures in the form of MFP and printer security features, Toshiba and 3rd party products, implementation services and training.

This document is targeted to end user decision makers and as such describes the business issues and Toshiba's comprehensive approach to remediation. Technical documentation and other white papers on various technologies and countermeasures are available upon request.

Businesses are at risk

Businesses are at risk.

Businesses are at risk from unsecured MFP and printer devices, weak access controls, unsecured documents and limited employment of end of life policies.

These risks broadly speaking can be identified firstly, as the leakage or theft of intellectual property, secondly, litigation resulting from non compliance with a broad range of federal, state, municipal and industry specific regulations and thirdly the damage to IT infrastructure and the denial of services and IT resource availability.

Data leakage, the loss of corporate knowledge cost US business $600 BN each year according to the association of certified fraud examiners. Counterfeiting and document fraud account for two thirds of the annual cost.
IT infrastructure, collaboration software and business applications are typically secured, however mfp and printer devices are often left unsecured and paper and electronic documents more often than not remain unsecured for the duration of their lifecycle. Documents 'at rest' in corporate email, shared drives or 'in transit' from pc to printer or from MFP to recipient are typically unsecured.

Litigation is increasing and the array of regulations that enterprises must adhere too are far reaching with significant penalty for non compliance up to and including incarceration. Frequently cited legislation includes HIPAA (Health Insurance Portability and Accountability Act), SOX (Sarbanes Oxley), FERPA (Family Education Rights and Privacy Act) and GLBA(GRAMM-Leach Bliley Act).

Malicious intrusion of corporate networks is on the rise with coordinated attacks by national intelligence services, crime syndicates and disgruntled employees.

Businesses are at risk

Businesses are at risk.

Unsecured MFP’s and printers can be exploited through open ports. Malicious intruders can gain access to latent document images on unsecured MFP’s and printers and potentially exploit other devices on the network such as PC’s and Servers. Unsecured MFP’s and printers can be used to attack the IT infrastructure through denial of service attacks and the deployment of malware such as viruses, bots and keystroke loggers to name a few.

MFP’s are often not securely accessed with user authentication and as such can be used to leak information or penetrate the network internally in the case of a disgruntled employee.

As with other areas of information technology, security needs to be applied to MFP, printer devices, and documents holistically and in depth or else organizations run the significant risk of data leakage, regulatory non-compliance and attacks on their IT infrastructure.

Encompass Security Solutions

Encompass Security Solutions.

Toshiba provides assessment services which provide a roadmap to remediate security vulnerabilities on MFP and printer devices, access controls, documents and end of life policies. Encompass Security Solutions include assessment services, security vulnerability countermeasures and training and are offered on Toshiba MFP's and on a variety of printer brands ensuring a comprehensive remediation strategy and providing for incorporation into a managed print services environment. SecureMFP is the brand Toshiba uses to describe security countermeasures and related products and services on Toshiba MFP's

Encompass Security Solutions group vulnerabilities and the respective countermeasures into 4 categories:

1) Device Security
2) Access Security
3) Document Security
4) End of Life Security

Through assessment, we are able to grade the security of your devices, access controls and document security as follows

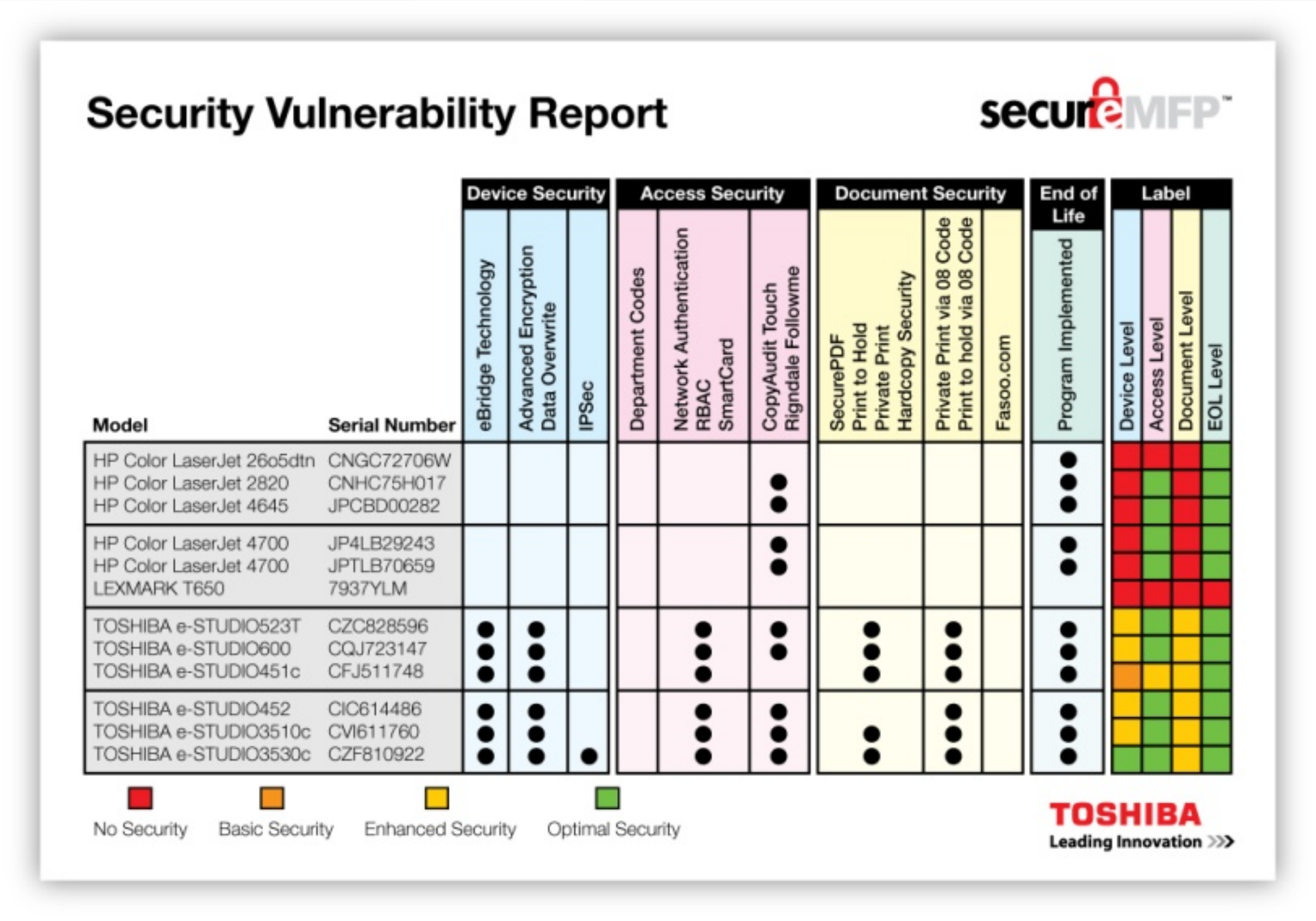
1) None
2) Basic
3) Enhanced
4) Optimal

Through consultation, our Toshiba Business Analysts will assess and develop a roadmap and Toshiba System Engineers will implement the recommendations by enabling and installing device, access and document security countermeasures.

Encompass Security Assessment

Encompass Security Assessment.

An example Encompass Security Assessment is provided below:



Security Vulnerability Report

secureMFP™

		Device Security			Access Security			Document Security			End of Life	Label			
Model	Serial Number	eBridge Technology	Advanced Encryption Data Overwrite	IPSec	Department Codes	Network Authentication RBAC SmartCard	CopyAudit Touch Rigndale Followme	SecurePDF Print to Hold Private Print Hardcopy Security	Private Print via 08 Code Print to hold via 08 Code	Fasoo.com	Program Implemented	Device Level	Access Level	Document Level	EOL Level
HP Color LaserJet 26o5dtn	CNGC72706W										●	🟥	🟥	🟥	🟩
HP Color LaserJet 2820	CNHC75H017						●				●	🟥	🟩	🟥	🟩
HP Color LaserJet 4645	JPCBD00282						●				●	🟥	🟩	🟥	🟩
HP Color LaserJet 4700	JP4LB29243						●				●	🟥	🟩	🟥	🟩
HP Color LaserJet 4700	JPTLB70659						●				●	🟥	🟩	🟥	🟩
LEXMARK T650	7937YLM											🟥	🟥	🟥	🟥
TOSHIBA e-STUDIO523T	CZC828596	●	●			●	●	●	●		●	🟨	🟩	🟨	🟩
TOSHIBA e-STUDIO600	CQJ723147	●	●			●	●	●	●		●	🟨	🟩	🟨	🟩
TOSHIBA e-STUDIO451c	CFJ511748	●	●			●		●	●		●	🟧	🟨	🟨	🟩
TOSHIBA e-STUDIO452	CIC614486	●	●			●	●		●		●	🟨	🟩	🟨	🟩
TOSHIBA e-STUDIO3510c	CVI611760	●	●			●	●	●	●		●	🟨	🟩	🟨	🟩
TOSHIBA e-STUDIO3530c	CZF810922	●	●	●		●	●	●	●		●	🟩	🟩	🟨	🟩

🟥 No Security 🟧 Basic Security 🟨 Enhanced Security 🟩 Optimal Security

TOSHIBA
Leading Innovation >>>

Countermeasures

Countermeasures

Vulnerabilities and their respective countermeasures are grouped into 4 categories and are typically additive:

Device Security – *Is data safe?*	**Document Security –** *Are documents protected?*
• SSL	• Private Print
• IPv6	• Print to Hold
• IP Filtering	• SecurePDF
• SMB Signing	• HardCopy Security
• IPSec	• Private Print (Policy)
• Advanced Encryption	• Print to Hold (Policy)
• Data Overwrite Kit	• Fasoo Digital rights Management
Access Security- *Is access locked down?*	**End of life Security? –** *Is disposal secure?*
• Department Codes	• Hard drive scrubbing/removal
• Strong Passwords	
• Usage Limitations	
• Job Log	
• LDAP Integration	
• Network Authentication w/RBAC	
• Email Authentication	
• SmartCard Authentication	
• Copy Audit Touch	
• Ringdale FollowME	
• Pharos Blueprint Enterprise	

Countermeasures

Device Security Countermeasures

Device Security - Is data safe?

- **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.

- **IPv6**
- *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

- **IP Filtering**
- *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

Device Security

Device Security Countermeasures

Device Security - Is data safe?

- **SMB Signing**
- *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.

- **IPSec**
- *IPsec* (IP Security Protocol) protects communication in theIP layer. Provides authenticated and encrypted submission of print jobs from desktop to Toshiba MFP's.

- **Advanced Encryption**
- *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 Kit

Device Security

Device Security Countermeasures

Device Security - Is data safe?

- **Data Overwrite Kit**
- *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.

Access Security

Access Security Countermeasures

Access Security - Is access locked down?

- **Department Codes**
- *User/Department 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.

- **Strong Passwords**
- *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

Access Security

Access Security Countermeasures

Access Security - Is access locked down?

- **Usage Limitations**
- *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.

- **Job Log**
  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.

- **Network Authentication w/RBAC**
- *Network Authentication* –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.

Access Security

Access Security Countermeasures

Access Security - Is access locked down?

- **Email Authentication**
- Authenticate natively with Microsoft Exchange email Servers

- **LDAP Integration**
- *Lightweight Directory Access Protocol (LDAP) Integration* – LDAP 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 integration 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.

- **SmartCard Authentication**
- *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.

- **Print Audit with Copy Audit Touch**
- Print tracking and cost accounting, secure release with copy audit touch

Access Security

Access Security Countermeasures

Access Security - Is access locked down?

- **Ringdale FollowME**
- Print tracking and cost accounting, follow me printing, secure release.

- **Pharos BluePrint Enterprise**
- Print tracking, print policy, cost accounting and , secure release pull printing.

Document Security

Document Security Countermeasures

Document Security - Are documents protected?

- **SecurePDF**
- *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.

- **Private Print**
- *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.

Document Security

Document Security Countermeasures

Document Security - Are documents protected?

- **HardCopy Security**
- Embedded pattern print is a security function, which effectively restrains unauthorized copying and prevents the leakage of information by embedding hidden character strings during printing which reveal themselves when the document is copied. Example – ‘Copying Prohibited’

- **Fasoo Enterprise Digital Rights Management**
- Digital rights management software for enterprises and for inter-enterprise document exchange

End of Life Security

End of Life Security Policy

End of Life Security Policy – Is disposal secure?

- **Hard Drive Scrubbing**
- It is important that organizations have a policy in place to ensure MFP and printer assets are scrubbed of sensitive data through hard drive scrubbing as devices reach their end of life or come to the end of the lease term.
- If no end of life policy exists, Toshiba will build one for you as part of an Encompass security vulnerability assessment.