TOSHIBA

Toshiba Insight | Security

How to protect your organisation's sensitive data:

– Access Security
– Document Security
– Device Security

TOSHIBA

01 What's the risk?

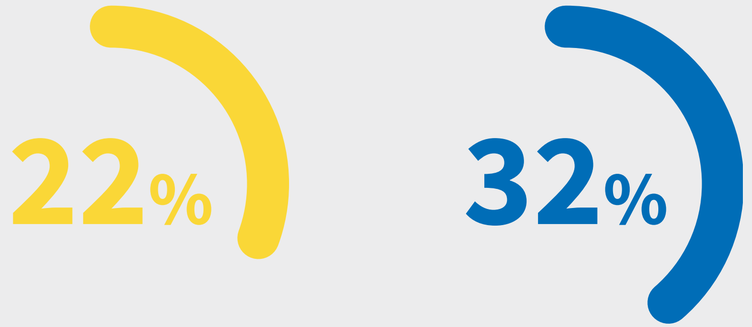
Why you should take security of your organisation's print infrastructure seriously.

[1)] Data taken from the Department of Media, Culture and Sport's 'Cyber Security Breaches Survey 2019'

Every day millions of confidential files – such as legal documents or financial data – are produced and distributed via multifunctional products (MFPs) and printers. With these devices being able to store large amounts of data on their hard drives, they have become an integral part of business networks and thus are a critical point of vulnerability. Sensitive data and business-critical information can easily be tampered with if security measures are not in place. However, although the vast majority of organisations secure their IT networks, the same level of attention is not being given to their print infrastructure. An insecure MFP leaves those working with sensitive information vulnerable to attack and at risk of prosecution if they do not keep their data safe. There are three areas you should look to secure in order to keep your documents safe:

- **Access Security**
- **Document Security**
- **Device Security**

Cyber security in 2019[1)]



of **businesses**/**charities** identified cyber security breaches or attacks in the last 12 months. The average annual cost for those that lost data or assets after breaches was:

£4,180 / £9,470

TOSHIBA

02 Access security.

You should look to control who, what, and how much.

Toshiba has developed simple yet highly effective methods of establishing access security without inconveniencing users.

User/Departmental 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. 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 unauthorised users from abusing company resources or gaining access to confidential information.

Strong Administrator Passwords | Unauthorised persons will find it more 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, a login limitation of up to three times can be employed – after which, the devices screen will be locked.

Network Authentication | For 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. If a user is authorised on the corporate network, then he or she can gain access to the MFP. Authentication ensures that only those users who have been authorised 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.

Card or Biometric Authentication | Card or biometric authentications offer extensive security features designed to eliminate unauthorised operation thereby reducing costs and downtime. By utilising a streamlined, single point of entry, it facilitates the user log-in process by requiring a card swipe or finger print scan instead of typing a user name and password.

E-mail Authentication | Authenticate natively with Microsoft Exchange e-mail servers.

Lightweight Directory Access Protocol (LDAP) Integration | LDAP provides a centralised 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.

Usage Limitations | Usage limitations allow the administrator to control and track output at the device, by setting limits for the number of copies or prints available at an account or a departmental level. The use of colour is also an optional restriction when dealing with a colour-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.

Furthermore, the user login process can be streamlined wth the use of optional card readers - these require a simple swipe of a card to provide user access to specific features and functions.

Certificates

Common Criteria Evaluated Assurance Level 3 (EAL 3)
The Common Criteria for IT Security Evaluation has different levels which describe in detail the requirements of an IT security inspection. The evaluation confirms that the security functionality stated by a manufacturer is valid. EAL3 evaluates the security behaviour of a device and uses development environment controls to confirm secure delivery procedures.

ISO/IEC 15408
Standard containing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.

IEEE 2600.1 standards
Standard for a Protection Profile for Hardcopy Devices in a restrictive commercial information processing environment in which a relatively high level of document security, operational accountability, and information assurance, are required. Typical information processed in this environment is trade secret, mission-critical, or subject to legal and regulatory considerations such as for privacy or governance. This environment is not intended to support life-critical or national security applications.

TOSHIBA

03 Document security.

How to protect documents which are for your eyes only.

Confidential data needs to be protected at all times. To ensure printed documents do not fall into the wrong hands, Toshiba offers the following solutions.

Private Print | This functionality offers complete control of print output, requiring users to input a password before their document is outputted from the machine. When users are at the device to retrieve their document, they first have to enter their individually selected confidential password or swipe their authentication card. Only then will the documents sent by the user be released.

Secure PDF | Much like the private print feature, further control and protection are needed when scanning documents to e-mail 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 AES encryption can be applied to ensure the document is protected.

Hard Copy Security | Embedded pattern print is a security function, which effectively restrains unauthorised 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.

Pull-Printing Solutions | Pull-printing solutions hold print jobs in a central queue until the user logs on to any pull-printing enabled MFP, ensuring that the correct user is physically present before the document is printed.

End of life security

Serious consideration also needs to be given to what happens to MFPs once they have reached their end-of-life and/or are taken off site. If the HDD falls into the wrong hands, the data stored on it is at stake.

Toshiba's innovative Secure Hard Disk Drive has set new security standards and provides ultimate security for sensitive data. The 256-bit AES encryption happens in near real-time and the encryption key is stored on the hard disc drive itself. Furthermore, the Toshiba Secure HDD knows which device it has been built into and requires the system to authenticate itself against the hard disc before allowing the data to be accessed. If this authentication fails, the encryption key will be deleted, guaranteeing that your data is safe.

And while in the past invalidating the data on an hard disk at the end of a products life-time was extremely time-consuming, Toshiba's Secure HDD puts an end to this. The data on the disk is safe forever.

All our e-BRIDGE Next MFPs are equipped with the Toshiba Secure HDD.

TOSHIBA

04 Device security.

Protecting you and your network.

MFPs and network printers function as complex network devices, Toshiba has developed several solutions that specifically address network security.

Secure Sockets Layer (SSL) | 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 fulfilment, and accessing online accounts. MFP devices employ this common encryption technology to protect all data travelling to and from the MFP. Print jobs sent via SSL are encrypted through symmetric cryptography, ensuring that the print data is secure and will not be used for any purpose other than print output.

IPv6 | IPv6 is the latest version of IP and offers several features to address IP security needs such as increased address size, built in support for authentication, and stronger confidentiality.

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 utilise this mechanism as a means of controlling which computers have access.

Server Message Block (SMB) Signing | SMB 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 the IP layer. It provides authenticated and encrypted submission of print jobs from desktop to a Toshiba MFP.

Advanced Encryption | Toshiba's innovative Secure Hard Disk Drive has set new security standards and provides ultimate security for sensitive data. The 256-bit AES encryption happens in near real-time and the encryption key is stored on the hard disc drive itself. Furthermore, the Toshiba Secure HDD knows which device it has been built into and requires the system to authenticate itself against the hard disc before allowing the data to be accessed. If this authentication fails, the encryption key will be deleted, guaranteeing that your data is safe.

Data Overwrite Kit | Data overwriting ensures that the hard drive is absolutely clear of readable data needed to process a print, scan copy or fax job. It works by overwriting the actual data with random and numerical characters. The disk is automatically cleared immediately after the device is done using the information after every job, thus preventing the data from being recovered by unauthorised users.

TOSHIBA

05 What to do next.

Discuss your print infrastructure with one of our consultants.

Toshiba work with business of all sizes, from small start-ups to global enterprises. Having worked across diverse and demanding sectors, we have the experience to help your business overcome technical challenges and flourish.

At Toshiba, we do not believe in ‘one size fits all’. Instead, we work with organisations to build bespoke solutions tailored to organisational needs. This helps our solutions seamlessly integrate into existing systems and workflows which minimises cost and disruption to you organisation.

To get started, we recommend a call with one of our experts to discuss the challenges your company is facing and the various options available to you to address these.

We look forward to helping your business with a secure, efficient and environmentally friendly print infrastructure.

Get in touch

Telephone
+44 (0)843 2244944

Email
info@toshibatec.co.uk

Website
www.toshibatec.co.uk