European Network and Information Security Agency

Secure printing

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and the private business and industry actors.

Contact details:

For contacting ENISA or for general enquiries on Member State awareness programmes, please use the following details:

e-mail: Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu
Internet: http://www.enisa.europa.eu/

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

enisa

European Network and Information Security Agency

Secure printing

April 2008

Contents

Executive summary

Business and transaction documents printed by suppliers or in captive printing and mailing operations are susceptible to security breaches, as recent news stories have highlighted.

This factor underlines the fact that document printing and copying are often mistakenly viewed as static or legacy work processes. New printing technologies and applications in fact are providing ways for companies to improve customer communications, cut spending and streamline business processes exposing organisations to security risks and threats ([1]). It is therefore crucial to employ good practice to comply with existing regulations and secure printed information ([2]).

Document security on printers and multifunction products is an issue within corporations ([3]). A data cartridge containing the pension details of more than 6,500 people has been mislaid by HM Revenue and Customs in United Kingdom (UK) ([4]). Furthermore in UK, confidential police documents including names, dates of birth, addresses and telephone numbers were found in the Hemlington area of Middlesbrough ([5]); documents containing payroll information relating to 182 NHS staff members were found dumped in a street ([6]). A California Public Employees' Retirement System mailing that exposed members' social security numbers underscores the need to place equal emphasis on securing business and customer data — whether it resides in data centres, networks, or print and mail operations ([7]).

Furthermore, top management sees protecting customer data as a very important driver of their expenditure ([8]). Thanks to managed print service, overall output costs spending on office print can be reduced by up to 30 % ([9]).

If we look at Europe, awareness of management of printing systems and strategies for deriving the greatest benefits from these services is low among more than 350 French, German and UK organisations ([10]). The scenario presents countless difficulties and must be taken seriously.

This document gives a brief outline of the data which is susceptible to security breaches/incidents, highlights potential risks associated with document printing and copying, and lists good practice guidelines which aim at helping readers to overcome secure printing obstacles within their organisations.

The document does not cover the legal aspect associated to this matter. Moreover, it should not be seen either as a comprehensive source of all risks associated with secure printing or a technical guideline to secure printing standards or solutions.

([1]) *Hype cycle for printing markets and management, 2005,* Peter J. Grant et al, Gartner, 21 June 2005.

([2]) *New attacks: device vulnerabilities stand out,* Avivah Litan, Don Dixon, Greg Young, Gartner, 7 December 2006.

([3]) *How to mitigate information loss on MFPs*, Don Dixon, Gartner, 26 April 2006.

([4]) *Pension details of 6,500 lost in new data fiasco*, Nick Allen and Gary Cleland, Telegraph.co.uk, 19 December 2007, available at http://www.telegraph.co.uk/news/uknews/1572917/Pension-details-of-6,500-lost-in-new-data-fiasco.html (visited on 22 April 2008).

([5]) *Police documents dumped in street*, BBC News, 11 January 2008, available at http://news.bbc.co.uk/2/hi/uk_news/england/tees/7183088.stm (visited on 22 April 2008).

([6]) *NHS staff documents found dumped*, BBC News, 28 March 2008, available at http://news.bbc.co.uk/2/hi/health/7319293.stm (visited on 22 April 2008).

([7]) *Information breach highlights production print and mail vulnerabilities*, Pete Basiliere, Gartner, 18 September 2007.

([8])*BERR 2008 Information Security Breaches Survey*, PricewaterhouseCoopers, United Kingdom, April 2008, available at www.security-survey.gov.uk (visited on 22 April 2008).

([9]) *Is managed print service right for your office?,* Ken Weilerstein, 16 December 2005.

([10]) *User survey: managed print services, Europe, 2005 (executive summary),* Cecile Drew, Malcolm Hancock, Gartner, 2 September 2005.

Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways.

The author wish to acknowledge and thank VigiTrust, Hewlett-Packard and BOC Information Technologies Consulting AG for the prompt support, valuable input and material provided for the compilation of this booklet.

Finally, we would like to acknowledge the individuals who contributed to this document with informal reviews, valuable insights, observations, suggestions and solutions. The content would be incomplete and incorrect without their help.

Document printing and copying

Printers and copiers produce the bulk of hardcopy business output, such as invoices, forms, tickets, statements, employee documents and customer data. Thus, often sensitive data is most vulnerable when in transit between a user's workstation or laptop and a printing device's output-tray — particularly if printed remotely. It is therefore crucial to emphasise that printing devices are a powerful link within the overall security chain, since multi-function printers (MFPs [11]) provide features such as scan-to-e-mail/fax. Despite this crucial role in handling often confidential information, these devices and the documents they produce remain largely unprotected, leaving business and transaction documents printed susceptible to security breaches.

This is why document security on printers and multifunction products is an issue with enterprises. IT managers should prepare themselves and their organisations to manage print in a proactive way [12].

A growing market

The market for printers, copiers and multifunction products in Europe, the Middle East and Africa grew by 6 % year on year in the second quarter of 2007, with shipments totalling 10.9 million units. End-user spending in euro grew by 5 %, thanks to strong demand for MFPs in some emerging markets [13].

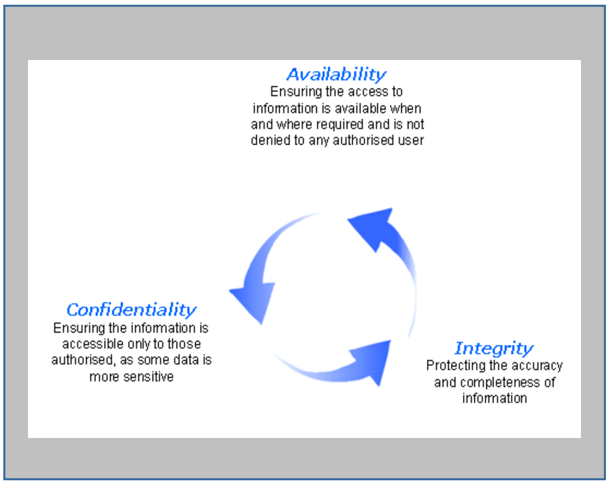
Secure printing

A definition

Secure printing is any step taken by an organisation to ensure that:

- ✓ printing devices will remain secure;
- ✓ printed or transmitted data will remain confidential, integral and available.

These three pillars or classifications of information security — confidentiality, availability and integrity — can be described as follows:


Availability
Ensuring the access to information is available when and where required and is not denied to any authorised user
Confidentiality
Ensuring the information is accessible only to those authorised, as some data is more sensitive
Integrity
Protecting the accuracy and completeness of information

Security standards

Having enterprises taking care of secure printing will help in complying with the three aspects of security (i.e. confidentiality, availability and integrity) and some security standards, such as the following.

[11] A typical MFP may act as a combination of some or all of the following devices: printer, scanner, photocopier, fax or e-mail.

[12] *What IT asset managers need to know about managing office print before it falls into their lap*, Ken Weilerstein, Gartner, 11 November 2005; *Secure printing solutions best practice – key concept, value add security advice for your organisation*, Hewlett-Packard, 2005.

ISO/IEC 17799:2005-06-15 (2nd edition)

ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

- ✓ security policy;
- ✓ organisation of information security;
- ✓ asset management;
- ✓ human resources security;
- ✓ physical and environmental security;
- ✓ communications and operations management;
- ✓ access control;
- ✓ information systems acquisition, development and maintenance;
- ✓ information security incident management;
- ✓ business continuity management;
- ✓ compliance.

The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 17799:2005 is intended as a common basis and practical guideline for developing organisational security standards and effective security management practices, and to help build confidence in interorganisational activities ([14]).

Best practices and controls related to secure printing matters

Of the best practices and controls mentioned above, several are relevant to secure printing, as follows:

- ✓ security policy;
- ✓ organisation of information security;
- ✓ asset management;
- ✓ physical and environmental security;
- ✓ communications and operations management;
- ✓ access control;
- ✓ information security incident management;
- ✓ business continuity management.

PCI data security standard (DSS)

The PCI DSS version 1.1 comprises a set of comprehensive requirements for enhancing payment account data security. This standard was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International to help facilitate the broad adoption of consistent data security measures on a global basis ([15]).

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organised, as follows:

Build and maintain a secure network

- ✓ Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- ✓ Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

- ✓ Requirement 3: Protect stored cardholder data
- ✓ Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

- ✓ Requirement 5: Use and regularly update anti-virus software
- ✓ Requirement 6: Develop and maintain secure systems and applications

Implement strong access control measures

[13] *Quarterly statistics: state of the printer, copier and MFP market, EMEA, 2Q07,* Sharon McNee, Cecile Drew, Tosh Prabhakar, Gartner, 10 September 2007.

[14] http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm (visited on 4 April 2008).

[15] https://www.pcisecuritystandards.org/tech/index.htm (visited on 14 April 2008).

- ✓ Requirement 7: Restrict access to cardholder data by business need-to-know
- ✓ Requirement 8: Assign a unique ID to each person with computer access
- ✓ Requirement 9: Restrict physical access to cardholder data

Regularly monitor and test networks

- ✓ Requirement 10: Track and monitor all access to network resources and cardholder data
- ✓ Requirement 11: Regularly test security systems and processes

Maintain an information security policy

- ✓ Requirement 12: Maintain a policy that addresses information security [16].

Principles and accompanying requirements related to secure printing matters

Of the principles and accompanying requirements mentioned above, only a few are relevant to secure a printing environment [17], as follows:

Protect cardholder data

- ✓ Requirement 3: Protect stored cardholder data
- ✓ Requirement 4: Encrypt transmission of cardholder data across open, public networks

Implement strong access control measures

- ✓ Requirement 7: Restrict access to cardholder data by business need-to-know
- ✓ Requirement 8: Assign a unique ID to each person with computer access
- ✓ Requirement 9: Restrict physical access to cardholder data

Maintain an information security policy

- ✓ Requirement 12: Maintain a policy that addresses information security

COBIT

COBIT is a framework and supporting tool set that allow managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders. COBIT enables the development of clear policies and good practice for IT control throughout enterprises. COBIT is continuously kept up to date and harmonised with other standards and guidance.

Hence, COBIT has become the integrator for IT good practice and the umbrella framework for IT governance that helps in understanding and managing the risks and benefits associated with IT. The process structure of COBIT and its high-level, business-oriented approach provide an end-to-end view of IT and the decisions to be made about IT [18].

COBIT IT processes related to secure printing issues

Of the COBIT IT processes, several are relevant to matters related to secure printing. As for COBIT the security of exchange of data is independent from the means used, secure printing is not explicitly mentioned in any process. However within the COBIT framework one main domain is relevant to secure printing: deliver and support (DS).

- ✓ *Deliver and support* [19]
  - DS5 Ensure systems security: Ensure systems security that satisfies the business requirement for IT of maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents by focusing on defining IT security policies, plans and procedures, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents is achieved by
    - Understanding security requirements, vulnerabilities and threats
    - Managing user identities and authorisations in a standardised manner
    - Testing security regularly.

[16] https://www.pcisecuritystandards.org/tech/index.htm (visited on 4 April 2008). For further information on the PCI standard please see http://www.pcistandard.com/ (visited on 4 April 2008).

[17] *The PCI standard and its implications for the security industry*, Mathieu Gorge, VigiTrust, Computer Fraud & Security, February 2006.

[18] *COBIT 4.1 Excerpt — Executive summary framework, http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172* (visited on 4 April 2008).

[19] *COBIT 4.1*, IT Governance Institute, USA, 2007.

Within this domain, five control objectives [20] were identified:

- DS5.3 Identity Management: Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.
- DS5.4 User Account Management: Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.
- DS5.11 Exchange of Sensitive Data: Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, and proof of receipt and non-repudiation of origin.

combined with:

- DS11.6 Security Requirements for Data Management: Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements
- DS12.3 Physical Access: Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.

Furthermore, the following domains and control objectives should be taken into consideration [21]:

✓ *Plan and organise*

- PO1 Define a strategic IT plan: Define a strategic IT plan that satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks by focusing on incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a

[20] Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected. IT control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process, *COBIT 4.1*, IT Governance Institute, USA, 2007.

[21] *COBIT 4.1*, IT Governance Institute, USA, 2007.

transparent and effective manner is achieved by

  - Engaging with business and senior management in aligning IT strategic planning with current and future business needs
  - Understanding current IT capabilities
  - Providing for a prioritisation scheme for the business objectives that quantifies the business requirements

- PO2.3 Data Classification Scheme: Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.
- PO2.4 Integrity Management: Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.
- PO4 Define the IT processes, organisation and relationship: Define the IT processes, organisation and relationships that satisfies the business requirement for IT of being agile in responding to the business strategy whilst complying with governance requirements and providing defined and competent points of contact by focusing on establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes is achieved by
  - Defining an IT process framework
  - Establishing appropriate organisational bodies and structure
  - Defining roles and responsibilities
- PO5 Manage the IT investment: Manage the IT investment that satisfies the business requirement for IT of continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardised services that satisfy end-user expectations by focusing on effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions is achieved by
  - Forecasting and allocating budgets
  - Defining formal investment criteria (ROI, payback period, net present value [NPV])
  - Measuring and assessing business value against forecast
- PO6 Communicate management aims and direction: Communicate management aims and direction that satisfies the business requirement for IT of supplying accurate and timely information on current and future IT services and associated risks and responsibilities by focusing on providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders, embedded in an IT control framework is achieved by
  - Defining an IT control framework
  - Developing and rolling out IT policies
  - Enforcing IT policies
- PO9 Assess and manage IT risks: Assess and manage IT risks that satisfies the business requirement for IT of analysing and communicating IT risks and their potential impact on business processes and goals by focusing on development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk is achieved by
  - Ensuring that risk management is fully embedded in management processes,

internally and externally, and consistently applied

    - Performing risk assessments
    - Recommending and communicating risk remediation action plans

- ✓ *Acquire and implement*
  - AI4 Enable operation and use: Enable operation and use that satisfies the business requirement for IT of ensuring satisfaction of end users with service offerings and service levels and seamlessly integrating applications and technology solutions into business processes by focusing on providing effective user and operational manuals and training materials to transfer the knowledge necessary for successful system operation and use is achieved by
    - Developing and making available knowledge transfer documentation
    - Communicating and training users, business management, support staff and operational staff
    - Producing training materials
- ✓ *Deliver and support*
  - DS1 Define and manage service levels: Define and manage service levels that satisfies the business requirement for IT of ensuring the alignment of key IT services with the business strategy by focusing on identifying service requirements, agreeing on service levels and monitoring the achievement of service levels is achieved by
    - Formalising internal and external agreements in line with requirements and delivery capabilities
    - Reporting on service level achievements (reports and meetings)
    - Identifying and communicating new and updated service requirements to strategic planning
  - DS4 Ensure continuous service: Ensure continuous service that satisfies the business requirement for IT of ensuring minimal business impact in the event of an IT service interruption by focusing on building resilience into automated solutions and developing, maintaining and testing IT continuity plans is achieved by
    - Developing and maintaining (improving) IT contingency
    - Training on and testing IT contingency plans
    - Storing copies of contingency plans and data at offsite locations
  - DS6 Identify and allocate costs: Identify and allocate costs that satisfies the business requirement for IT of ensuring transparency and understanding of IT costs and improving cost-efficiency through well informed use of IT services by focusing on complete and accurate capture of IT costs, a fair system of allocation agreed upon by business users, and a system for timely reporting of IT use and costs allocated is achieved by
    - Aligning charges to the quality and quantity of services provided
    - Building and agreeing on a complete cost model
    - Implementing charges as per the agreed-upon policy
  - DS7 Educate and train users: Educate and train users that satisfies the business requirement for IT of effectively and efficiently using applications and technology solutions and ensuring user compliance with policies and procedures by focusing on a clear understanding of IT user training needs, execution of an effective training strategy and measurement of the results is achieved by
    - Establishing training curricula
    - Organising training
    - Delivering training
    - Monitoring and reporting on training effectiveness
  - DS8 Manage service desk and incidents: Manage service desk and incidents that satisfies the business requirement for IT of enabling effective use of IT systems by

ensuring resolution and analysis of end-user queries, questions and incidents by focusing on a professional service desk function with quick response, clear escalation procedures, and resolution and trend analysis is achieved by

  - Installing and operating a service desk
  - Monitoring and reporting trends
  - Defining clear escalation criteria and procedures

- DS9 Manage the configuration: Manage the configuration that satisfies the business requirement for IT of optimising the IT infrastructure, resources and capabilities, and accounting for IT assets by focusing on establishing and maintaining an accurate and complete repository of asset configuration attributes and baselines, and comparing them against actual asset configuration is achieved by
  - Establishing a central repository of all configuration items
  - Identifying configuration items and maintaining them
  - Reviewing integrity of configuration data
- DS10 Manage problems: Manage problems that satisfies the business requirement for IT of ensuring end users' satisfaction with service offerings and service levels, and reducing solution and service delivery defects and rework by focusing on recording, tracking and resolving operational problems; investigating the root cause of all significant problems; and defining solutions for identified operations problems is achieved by
  - Performing root cause analysis of reported problems
  - Analysing trends
  - Taking ownership of problems and progressing problem resolution
- DS13 Manage operations: Manage operations that satisfies the business requirement for IT of maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures by focusing on meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring and maintaining infrastructure is achieved by
  - Operating the IT environment in line with agreed-upon service levels and defined instructions
  - Maintaining the IT infrastructure.

Identifying corporate assets and their value

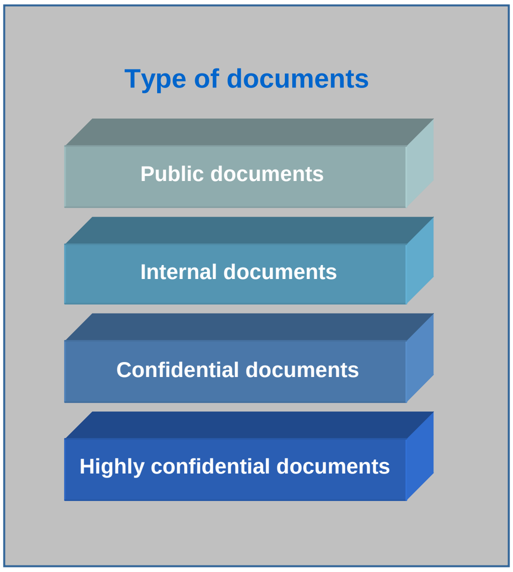
The following corporate assets were identified in terms of secure printing:

- ✓ physical assets: printing, fax, email devices;
- ✓ people: employees, contractors, visitors;
- ✓ software: intellectual property rights (IPR) and patents;
- ✓ data printed, copied and transmitted.

Major dangers for secure printing assets

An uncontrolled printing environment is a major danger. Thus the following should be taken into consideration for securing printing assets:

- ✓ location of network/local printers: printing devices located in public areas are accessible by staff, contractors, visitors and they are remote from staff desktops in most cases;
- ✓ access: who is allowed to print, scan and copy documents;
- ✓ type of documents which are printed, scanned, copied: public documents, internal documents, confidential documents, highly confidential documents. According to the different industry sectors — bank, insurance etc. — the confidential documents which may be printed are different.



- ✓ costs and ROI: increase costs and eventual impossibility to achieve return on investment.

Risks

Looking at the uncontrolled printing environment, the following risks can be identified ([22]):

- ✓ damage to company reputation: when either printed/copied/scanned information is stolen and used to damage the reputation of the company;
- ✓ damage to business: when either printed/copied/scanned information is stolen and used to damage the business of the company;
- ✓ damage to company image: when either printed/copied/scanned information is stolen and used to damage the image of the company;
- ✓ printed documents going missing;
- ✓ printed documents forgotten in printer's output-tray;
- ✓ forgetting which documents were printed;
- ✓ other colleagues seeing information, eventually marked as confidential;
- ✓ information falling into the wrong hands: circulation of documents;
- ✓ breaches of copyright: users disseminate documents with IPR breaching copyright;
- ✓ information available in hard copy allowed to be circulated in soft copy as possible scan data;
- ✓ use of unauthorised printing devices on the corporate network ([23]): there are solutions on the market which allow administration to control and monitor the installation and use of devices and their number;
- ✓ security incidents (e.g. denial of service/mechanism attack etc.): printing devices can be used as a platform for denial of service attacks or other malicious activities. One of the examples is that default administrative access settings as Telnet ([24]), SNMP ([25]), FTP ([26]) and HTTP ([27]) are open to most printers, thus allowing hackers to
  - use printing devices to penetrate the network,
  - set themselves up as an administrator,
  - change the settings,
  - look for stored documents,
  - print out data on printing devices,
  - replay print jobs or other jobs stored on the MFP
  - use and configure network printers,
  - launch further attacks,
  - sniffing print jobs and replaying them,
  - hack the admin welcome page;
- ✓ fraud/deception;
- ✓ sabotage;
- ✓ extortion;
- ✓ identity theft;

[22] *Secure printing solutions best practice – key concept, value add security advice for your organisation*, Hewlett-Packard, 2005.

[23] *Small office/home office LANs face network access security challenges*, John Girard, Gartner, 6 July 2005.

[24] Telnet (TELecommunication NETwork) is a network protocol used on the Internet or local area network (LAN) connections.

[25] The simple network management protocol (SNMP) is part of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

[26] The file transfer protocol (FTP) is a network protocol used to transfer data from one computer to another through a network, such as over the Internet.

[27] Hypertext transfer protocol.

- ✓ spam;
- ✓ cost increase;
- ✓ availability of information on how to exploit printers from public websites (e.g. www.irongeek.com);
- ✓ terrorism.

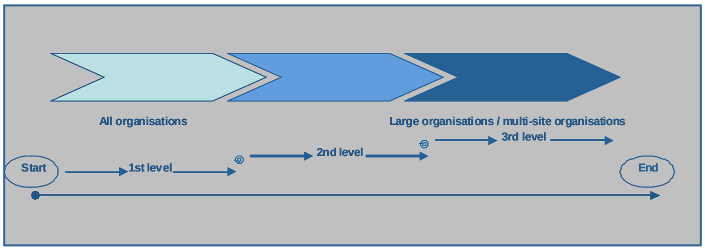
Our guidelines

Based on the data gathered and their analysis, this document provides good practice guidelines that can help readers and their organisations mitigate risks while dealing with secure printing matters.

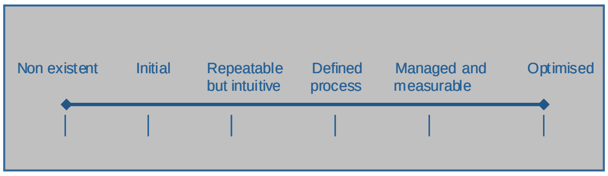
The good practice guidelines comprise:

- ✓ recommendations, and
- ✓ a checklist ([28]).

A multi-level approach identified allows organisations of different sizes (e.g. small and medium enterprises or multinational companies) and multiple sites to mitigate the risks mentioned above.



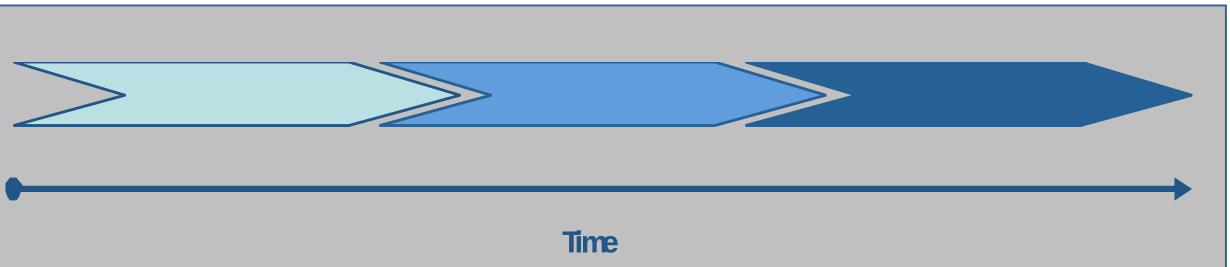
Another dimension which should be taken into considerations is the level of maturity of the processes in place in an organisation to mitigate risks related to secure printing. The maturity models can be represented as follows ([29]):



It is recommended to large or multi-site organisations to invest in a more complex and lengthy strategy to create a secure printing environment since the number of risks they may encounter may be greater than those of other enterprises.

[28] *Printing Environment Questionnaire,* VigiTrust Ltd., Dublin, 2006.
[29] *COBIT 4.1*, IT Governance Institute, USA, 2007.

Recommendations



✓ Define roles and responsibilities in relation to printing devices (i.e. RACI chart)

✓ Define procedures to guarantee a secure printing environment

✓ Do not consider corporate printers as
a mere IT service

✓ Avoid printing sensitive data if not necessary

✓ Locate corporate printers in protected or secured areas

✓ Control and monitor the installation and use of network printers

✓ Control printing environments

✓ Define a policy to guarantee a secure printing environment

✓ Increase IT support

✓ Implement security solution allowing limited number of users to print certain type of documents on designated secure printers

✓ Implement a full audit/tracking mechanism for printed jobs especially for organisations where service users (e.g. customers, students, third party) may be given credential to print jobs on the corporate network

✓ User authentication: 53 % of large companies use strong authentication for at least some of their systems as PIN codes, smartcards and biometric credentials. Some use two factor authentication addressing in this way the issue of unauthorised dissemination of IPR and breach of copyright.

✓ Define a secure printing strategy

✓ Deploy solutions allowing print jobs to be stored encrypted on a central server or at the printer whilst user goes to the printer to authorise the actual print-out. This will allow users to call the print job from multiple devices as long as they have the right credentials

✓ Call print jobs from different printing devices for roaming printing devices

✓ Implement a full audit/tracking mechanism for printed jobs. This will be difficult for job printed locally. This can lead to an accountability issue

✓ Infrastructure and operations managers must have business interruption recovery strategies for the printed documents critical to their enterprises' operations

✓ Encrypting information

Checklist

No	Checklist item
1.	☑ **Define a document flow and management**. A document flow and management is critical to the success of any secure printing strategy/policy/procedure. Assuming that confidential material is produced/received within the organisation, the following should be defined and monitored: ✓ number/type OR number/category of employees/users allowed to print/copy/scan documents / total number of employees/users; ✓ number/type OR number/category of employees/users allowed to use scan-to-fax/email/print feature / total number of employees/users; ✓ number of corporate policies referring to specific restrictions as to what may be printed/copied/scanned / total number of corporate policies; ✓ number of procedures to track printed/copied/scanned documents / total number of security procedures; ✓ number of reports on usage of printing devices per year.
2.	☑ **Ensure physical security of printing devices**. It is imperative to have up-to-date information on your printing environment and ensure that all possible actions to guarantee physical security of printing devices are taken. The following indicators can be used: ✓ number of printing devices per organisation; ✓ number of local devices / network devices in percentage; ✓ total number of MFP devices / total number of printing devices in percentage; ✓ number of printing devices located in a public area / total number of printing devices; ✓ number of printing devices located in a secured area / total number of printing devices; ✓ number of printing devices physically secured / total number of printing devices; ✓ number of hard disks easily removed from printing devices / total number of printing devices; ✓ number of hard disks taken away / total number of printing devices; ✓ number of stolen printing devices / month.
3.	☑ **Ensure printing device logical security (network, maintenance and access security aspects)**. Logical security covers software-based security settings, including username, password, authentication, access rights and privileges. The following should be checked to ensure logical security is guaranteed: ✓ number of users allowed to send printer job language (PJL) commands (30) which could reconfigure the printing devices / total number of users; ✓ number of printing devices requiring authentication to retrieve jobs / total number of printing devices; ✓ number of printing devices requiring authentication to scan-to-fax / total number of printing devices; ✓ number of printing devices requiring authentication to scan-to-email / total number of printing devices; ✓ number of printing devices requiring authentication to scan-to-print / total number of printing devices; ✓ number of users using smartcard as authentication mechanisms / total number of users; ✓ number of users using biometric as authentication mechanisms / total number of users; ✓ number of users using PIN code as authentication mechanisms / total number of users; ✓ number of users using building access/entry card as authentication mechanisms / total number of users; ✓ number of reports available out of the box to track authentication and related usage / month; ✓ number of users using other mechanism as authentication / total number of users; ✓ number of hard disks with access rights / total number of hard disks; ✓ number of ports open / total number of ports; ✓ number of printing devices with access restriction / total number of printing devices; ✓ number of multi-site pull printing within corporate network / total number of multi-sites;

(30) For more information on PJL, refer to *Printer job language technical reference manual HP*, 10th edition — October 1997 (P/N 5021-0380), available at http://lprng.sourceforge.net/DISTRIB/RESOURCES/DOCS/pjltkref.pdf (visited on 14 April 2008).

No	Checklist item
	✓ number of controls in place to monitor pull printing activity / total number of security controls; ✓ possibility to integrate existing user hierarchical structure into the printing environment (e.g. through LDAP (31) or MS Active Directory ® (32) in percentage.
4.	☑ **Ensure security of print data on hard disk or sent-to-printing devices**. It is very important to look at the format in which data is sent on printing devices and verify if print data residing on hard disks is stored and can be sniffed across the network. Moreover, it is recommended to check the following: ✓ number of hard disks used in printing devices / total number of printing devices; ✓ number of users allowed to access/read/modify data held on printer hard disks / total number of users; ✓ number of data held on printer hard disks purged / day; ✓ frequency of printing jobs / each MFP hard drive; ✓ number of data held on printer hard disks purged / week; ✓ number of printing devices which can hold data on their hard disk using fast unsecure purge (33) / total number of devices; ✓ number of printing devices which can hold data on their hard disk using fast secure purge (34) / total number of devices; ✓ number of printing devices which can hold data on their hard disk using secure purge (35) / total number of devices; ✓ number of printing devices which can hold data on their hard disk using other mechanism / total number of devices.
5.	☑ **Check how resilient your printing environment is**. It is crucial to understand how a business is dependent on the printing infrastructure and the availability of printing devices and its functionality is monitored and with what frequency. It is recommended to have an SLA for the maintenance/replacement of the printing devices. For large organisations, it is important to have an incident response plan covering the escalation of printing devices failure.
6.	☑ **Track printed copied and scanned documents to fax and email**.
7.	☑ **Establish a reporting flow on printing jobs**.
8.	☑ **Define a corporate policy or procedures to govern the use of printing devices**. In the policy, specify the users who are allowed to print/copy/scan documents, ensuring that they will be able to have access to the right information at the right time. Credentials must be communicated to the interested users.
9.	

[31] Lightweight directory access protocol is an application protocol for querying and modifying directory services running over TCP/IP.

[32] For organisations that require flexible support for directory-enabled applications, Microsoft has developed active directory application mode (ADAM). ADAM is a lightweight directory access protocol (LDAP) directory service that runs as a user service, rather than as a system service. Active directory application mode represents a breakthrough in directory services technology that provides flexibility and helps organisations avoid increased infrastructure costs. For more information, refer to http://www.microsoft.com/windowsserver2003/adam/default.mspx (visited 14 April 2008).

[33] Simple file table erase. Access to the file is removed but actual data is retained on the disk until it is overwritten by subsequent data storage operations. Usually it is the default erase mode.

[34] Access to the file is removed and the data is overwritten with a fixed character pattern.

[35] Similar to secure fast erase mode, but data is repetitively overwritten using an algorithm that prevents any residual data persistence. This mode may impact performance.

No	Checklist item
	☑ **Organise awareness training**. Training sessions could increase awareness of how a controlled printing environment can increase corporate security levels and productivity and reduce costs. Suggestions to promote awareness of good practice use of printing and document capture environments include face to face awareness sessions, e-learning based solutions as well as blended security learning services.
10.	☑ **Establish a secure printing strategy or include the printing environment in the overall security strategy of your organisation.** A strategy should be based on threat dynamics rather than internal company structure. Ensure the strategy is clearly defined and applied globally in the organisation. Ensure the strategy covers the technical, operational, commercial and legal aspects of the security. All secure printing initiatives will enhance efficiency and impact if part of a strategy.
11.	☑ **Obtain appropriate management support and funding**. Get stakeholder/senior management buy-in and support.
12.	☑ **Define goals and objectives**. In order to effectively plan, organise and evaluate a secure printing strategy, goals and objectives need to be identified. Encourage secure printing culture.
13.	☑ **Define target groups**. It is critical to identify users targeted by the strategy (i.e. staff; contractors, users).
14.	☑ **Select a solution and define procedure**. After careful evaluation, select the best solutions to implement the strategy. This is particularly critical for multi-site organisations.
15.	☑ **Develop a communications concept**. An effective and efficiently implemented communication plan is critical to the success of the strategy. The content of messages needs to be developed and tested, and appropriate communication channels identified. Ensure the strategy is communicated and contained within the staff handbook. Ensure thorough communications to gain cooperation and engagement from all.
16.	☑ **Define indicators to measure the success and benefits of the secure printing strategy**. It is imperative to clearly identify and construct metrics and key performance indicators.
17.	☑ **Establish baseline for evaluation**. Apart from identifying metrics and key performance indicators, the current situation with regards to the printing environment needs to be understood. This way, the effectiveness of the strategy can be measured based on the change in landscape.
18.	☑ **Document lessons learned**. Get the management and teams involved in capturing lessons learned from activities completed. It is therefore crucial to have the mandate and duty to report.

Benefits

An overview of the many benefits linked to a secure printing environment will help and lead the enterprises to better decide about this matter. The following benefits were identified:

- ✓ increased security;
- ✓ increased flexibility associated with solutions;
- ✓ decreased printing costs (e.g. money spent/device; ratio user/device and user/printing supplies (paper and ink); staff; maintenance) — for example by eliminating banner pages print managers can significantly reduce organisations' use of paper, saving up to 20 % in printing consumables (36). Gartner calculated that organisations can save 10 % to 30 % of their office printing spending, but only after they overcome certain obstacles ([37]);
- ✓ reduction of fraud cases;
- ✓ improved ROI;
- ✓ increased mobility and flexibility of users, turning what used to be a cost centre to a business enabler;
- ✓ achieve compliance (e.g. security audits against standards such as ISO 27002 or PCI DSS);
- ✓ enforcement of network central controls;
- ✓ full traceability of jobs;
- ✓ flexibility in revoking or granting rights to users (feature management);
- ✓ decrease number of incidents reported to IT related to printing issues
- ✓ overall alignment of printing environment with confidentiality, integrity and availability best practice security model.

Conclusions

Printing devices are handling often confidential information, such as invoices, forms, employee documents and customer data. These devices and the documents they produce remain largely unprotected, leaving as a result business and transaction documents printed susceptible to security braches. It is therefore crucial to underscore that printing devices are a powerful link within the overall security chain, since MFPs provide features as scan to e-mail/fax.

It is therefore crucial that IT asset managers prepare themselves and their organisations to manage print in a proactive way as ensuring a secure printing environment is key for any organisation regardless of its size and maturity.

Security of printing and document capture environments is an integral part of the organization overall security strategy.

ENISA hopes this booklet will provide enterprises with a valuable tool to take the first steps towards the preparation and implementation of a secure printing strategy.

([36]) *Eliminate banner pages and save up to 20 % in printing consumables*, Federico De Silva Leon, Charles Smulders, Ken Weilerstein, Gartner, 10 October 2007.

([37]) *Q&A for overcoming obstacles in managing office printing*, Ken Weilerstein, Gartner, 28 March 2008.

References and sources for further reading

1 - *Hype Cycle for Printing Markets and Management, 2005,* Peter J. Grant, Jim Tully, Rafe John Graham Ball, Andrew Kim, Lai-ling Lam, Federico De Silva Leon, Sharon McNee, Cecile Drew, Malcolm Hancock, Ken Weilerstein, Lynn Ritter, Don Dixon, Dan Sommer, David W. Haueter, Andrew Johnson, Tomoko Mitani, Gartner, 21 June 2005.

2 - *New Attacks: Device Vulnerabilities Stand Out,* Avivah Litan, Don Dixon, Greg Young, Gartner, 7 December 2006.

3 - *How to Mitigate Information Loss on MFPs*, Don Dixon, Gartner, 26 April 2006.

4 - *Pension details of 6,500 lost in new data fiasco*, Nick Allen and Gary Cleland, Telegraph.co.uk, 19 December 2007, available at http://www.telegraph.co.uk/news/uknews/1572917/Pension-details-of-6,500-lost-in-new-data-fiasco.html (visited on 22 April 2008).

5 - *Police documents dumped in street*, BBC News, 11 January 2008, available at http://news.bbc.co.uk/2/hi/uk_news/england/tees/7183088.stm (visited on 22 April 2008).

6 - *NHS staff documents found dumped*, BBC News, 28 March 2008, available at http://news.bbc.co.uk/2/hi/health/7319293.stm (visited on 22 April 2008).

7 - *Information Breach Highlights Production Print and Mail Vulnerabilities*, Pete Basilere, Gartner, 18 September 2007.

8 - *BEER 2008 Information Security Breaches Survey*, PricewaterhouseCoopers, United Kingdom, April 2008, available at www.security-survey.gov.uk

9 - *Is Managed Print Service Right for Your Office?,* Ken Weilerstein, 16 December 2005.

10 - *User Survey: Managed Print Services, Europe, 2005 (Executive Summary),* Cecile Drew, Malcolm Hancock, Gartner, 2 September 2005.

11 - *What IT Asset Managers Need to Know About Managing Office Print Before It Falls Into Their Lap*, Ken Weilerstein, Gartner, 11 November 2005.

12 - *Secure printing solutions best practice – key concept, value add security advice for your organisation*, Hewlett-Packard, 2005.

13 - *Quarterly Statistics: State of the Printer, Copier and MFP Market, EMEA, 2Q07,* Sharon McNee, Cecile Drew, Tosh Prabhakar, Gartner, 10 September 2007.

14 - http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm (visited on April 4th, 2008).

15 - http://www.pcistandard.com/pcistandard.html (visited on April 4th, 2008).

16 - *The PCI standard and its implications for the security industry*, Mathieu Gorge, VigiTrust, Computer Fraud & Security, February 2006.

17 - *COBIT 4.1 Excerpt – Executive Summary Framework, http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172 (visited on April 4th, 2008).*

18 - *COBIT 4.1*, IT Governance Institute, USA, 2007.

19 - *Small Office/Home Office LANs Face Network Access Security Challenges,* John Girard, Gartner, 6 July 2005.

20 - *Printing Environment Questionnaire*, VigiTrust Ltd., Dublin, 2006.

21 - *Printer Job Language Technical Reference Manual HP*, Tenth Edition — October 1997 (P/N 5021-0380), available at http://lprng.sourceforge.net/DISTRIB/RESOURCES/DOCS/pjltkref.pdf (visited on 14 April 2008).

22 - *Eliminate Banner Pages and Save Up to 20% in Printing Consumables*, Federico De Silva Leon, Charles Smulders, Ken Weilerstein, Gartner, 10 October 2007.

23 - *Q&A for Overcoming Obstacles in Managing Office Printing*, Ken Weilerstein, Gartner, 28 March 2008.

24 - *What developments can we expect regarding PCI DSS in 2008?*, Mathieu Gorge, Middle Ground, 2007.

European Network and Information Security Agency
P.O. Box 1309
71001 Heraklion
Greece
Tel: +30 2810 39 1280
http://www.enisa.europa.eu