Title:	Security of Paper Documents in the Workplace - Larry Ponemon - Ponemon Institute
Date:	11/17/08
Business Activities:	Data Management - Destruction, Employee Authentication, Security - Administrative Safeguards, Security - Physical Safeguards
Impact to Subscriber:	Insight into where and why paper documents are more at risk than electronic documents; ten recommendations to protect confidential and sensitive documents.

Authority: ★

Risk Guidance: ★★★★

Control Guidance: ★★★★

Relevance:

Background Facts:

- the Alliance for Secure Business Information (ASBI) sponsored a Ponemon Institute study on data breaches involving paper documents:
  - the 819 respondents work in IT operations, IT security, data protection and compliance departments in large organizations.

Relevance to Business Activities:

- **security - physical safeguards** considerations:
  - the risk of having sensitive and confidential paper documents lost or stolen is not going away:
    - despite widespread computer use, we still seem dependent on paper; and
    - 65% surveyed state the availability and use of paper documents has stayed the same or increased during the past two years.
  - this study dispels the myth that the cause of most data breaches is lost or stolen electronic documents:
    - 80% of respondents reported that their organization had one or more data breaches in the last 12 months:
      - 49% involved the loss or theft of paper documents.
    - 71% of respondents' organizations had lost or misplaced sensitive paper documents;
    - 53% believe that employees are putting paper documents at risk:
      - at communal printers;
      - in meeting rooms; or
      - at meetings held outside the office.
  - why businesses are at risk of data breaches involving paper documents:
    - there are not enough resources and controls available to secure paper documents:
      - 61% strongly agree or agree;
      - 23% are unsure; and
      - 16% strongly disagree or disagree.
    - controlling access to paper documents is harder than controlling access to electronic documents:
      - 57% strongly agree or agree;
      - 20% are unsure; and
      - 24% strongly disagree or disagree.
    - paper documents contain sensitive or confidential business information:
      - 59% strongly agree or agree;
      - 32% are unsure; and
      - 9% strongly disagree or disagree.
    - employees or contractors recognize what types of information are sensitive or confidential:
      - 35% strongly disagree or disagree;
      - 51% are unsure; and
      - 14% strongly agree or agree.
    - there is a risk that employees or contractors would have access to sensitive or confidential paper documents:
      - 21% strongly agree or agree;
      - 46% are unsure; and
      - 33% strongly disagree or disagree.
    - there is a strict policy for securing paper documents:
      - 22% strongly disagree or disagree;
      - 41% are unsure; and
      - 37% strongly agree or agree.
  - certain functions and types of information are believed to be more at risk because of the inability to secure paper documents:
    - the departments or functions most at risk are:
      - human resources (45%);
      - finance and accounting (40%);
      - information technology (38%);
      - sales (34%);
      - marketing (17%); and
      - legal and compliance (11%).
    - the top five types of information employees consider to most at risk are:

- employee records;
- customer information;
- management accounting reports and budgets;
- marketing and sales reports; and
- pre-released financial information and forecasts.

- paper documents are most at risk:
  - in a trash bin (62%);
  - when initially printed and in a communal printing tray (46%);
  - at an office desk (44%);
  - awaiting disposal or shredding (31%);
  - in a document archive or permanent storage (30%);
  - in the process of being circulated internally or mailed (18%);
  - in a filing cabinet (12%); and
  - before the document is printed and is in electronic format (6%).

- the amount of the organizations' sensitive or confidential information contained within paper documents is:
  - zero (5%);
  - less than 10% (9%);
  - less than 30% (18%);
  - less than 50% (11%); or
  - more than 50% (56%).

- in general, organizations are better able to govern the use, protection and disposal of electronic documents than physical:
  - organizations seem to be almost equally good at communicating data breaches involving both paper and electronic documents (72% vs. 64%), however:
    - organizations believe they are better at safeguarding electronic documents than paper documents, such as:
      - educating employees about access procedures:
        - 45% for electronic documents; and
        - 21% for paper documents.
      - assigning access rights based on an individual's role:
        - 45% for electronic documents; and
        - 18% for paper documents.
      - keeping logs about who is accessing information:
        - 43% for electronic documents; and
        - 11% for paper documents.
  - organization confidence level in their visibility to all users of sensitive information contained in paper documents and electronic files:
    - very confident:
      - 7% for electronic documents; and
      - 3% for paper documents.
    - confident:
      - 21% for electronic documents; and
      - 12% for paper documents.
    - somewhat confident:
      - 43% for electronic documents; and
      - 32% for paper documents.
    - not confident:
      - 29% for electronic documents; and
      - 53% for paper documents.
  - organizations suffer significant economic impact when paper documents are lost, missing or stolen:
    - 84% of organizations believe that as result of losing paper documents, they lost:
      - time;
      - money; and
      - other resources.
    - 46% surveyed estimate the financial impact to be between $10 million to $30 million per year;
    - root causes for financial loss due to loss or theft of paper documents containing sensitive information:
      - loss of personal information of customers (31%);
      - loss of competitive information (29%);
      - loss of trade secrets (26%);
      - loss of personal information about employees (5%);
      - loss of accounting or financial information (3%);
      - loss of information about vendors, contractors and customers (3%).

- **security - administrative safeguards** and **employee authentication** considerations:
  - not controlling access to paper documents with sensitive and confidential information increases the risk of a data breach:
    - employees, temporary employees or contractors have access to paper documents not pertinent to their role or responsibility:
      - never (8%);
      - sometimes (20%);
      - often (38%);
      - very often (9%); and
      - unsure (25%).
  - 55% of respondents were uncertain about who is accountable for granting access to paper documents:
    - accountability was attributed to:
      - business unit leaders (52%);
      - human resources department (31%);
      - legal, risk or compliance department (22%);
      - information technology department (15%); or
      - information security department (12%).

- 78% of organizations have a policy explaining how paper documents with sensitive data should be secured and disposed of safely, however:
  - only 29% of employees receive training about:
    - the policy; and
    - what types of information might be considered sensitive or confidential.
- recommendations to protect confidential and sensitive documents:
  - strict policies describing how sensitive and confidential documents should be disposed of;
  - strict enforcement of non-compliance with document handling and disposal procedures;
  - shredding machines that are easily accessible by employees;
  - senior level executive support;
  - ample budget to manage and control sensitive paper documents;
  - rigorous compliance of procedures for monitoring document protection and safe disposal;
  - establish accountability to business unit leaders to secure paper documents and files;
  - identification of areas on the organization that is most vulnerable and make sure there are procedures to properly dispose of paper documents;
  - training and awareness of what information the organization designates as confidential and sensitive; and
  - programs to train employees, contractors and third parties on the policies and their role in disposing of sensitive and confidential information.

- **data management - destruction** considerations:
  - the amount of paper documents containing confidential information that are shredded before disposal:
    - none are shredded (23%);
    - less than 10% (49%);
    - less than 30% (63%); and
    - less than 50% (77%).
  - the relatively low percentage of shredded documents suggests organizations are at risk for failing to secure sensitive or confidential information;
  - common steps taken to dispose of paper documents:
    - shredding documents in each office area (35%);
    - collecting documents from each office area for centralized off-site shredding (33%);
    - collecting documents from each office area for centralized in-house shredding (29%);
    - training employees about secure disposal (21%);
    - automated print restriction on specific devices (19%);
    - collecting paper documents from outside vendors for safe disposal (18%);
    - enforcing a policy on secure disposal (13%); and
    - automated print restrictions on specific files (3%).

Source Document:

http://www.fellowes.com/asbi/content/ASBI_SecurityofDocuments_Report.pdf