■ Paper as a Secure Form of Documentation & Communication

Paper is a secure form of documentation and communication in more than one sense. First, it is a secure format for storing information for the long term. It does not easily break down or fall apart over time and can last for centuries. The only equipment you need to retrieve the information stored on paper is your eyes – no source of electricity, computer or internet connection required. Second, personal and business information is generally more secure on paper, where it is safe from hackers and computer viruses. Consumers are concerned about the increasing number of data breaches at organizations that store personal information electronically that can lead to identity theft and fraud. Businesses, too, are concerned about data breaches and theft of their information assets. It is no wonder that many people prefer to receive financial materials in print rather than electronically. Third, electronic copies of important financial records supplied by banks and credit card companies may only be available for a finite time versus paper copies of these records, which can be kept safe and accessible in home filing systems.

- Digital storage media needs to be monitored for physical degradation over time.

    - The equipment needed to access the information stored on digital media needs to be kept in working order.

    - As software, operating systems and hardware change over time, the data stored on digital media needs to be updated or migrated to other media formats to ensure it can continue to be accessed.

    - Other concerns with digital storage media include: the loss of functionality of access drives; the need for both analog and digital backups; the obsolescence of data formats, storage media, and the equipment necessary to access the data; media and hardware failures; software failures; communication channel errors; and network service failures. (Gladney, 2007; Ross, 2012)

Information stored on paper is easily accessible and does not need extensive ongoing monitoring. With digital storage media, however, the need for machinery and software to access the data requires ongoing maintenance.

Nearly two thirds of all Americans and three quarters of Millennials have fallen victim to some type of cybercrime.

- According to research conducted by computer security giant Norton, in 2011, 431 million adults in 24 countries were victims of cybercrime, and over 1 million people become victims each day. (Norton, 2012)

- 54% of survey respondents have had their computers infected by malware and/or viruses; 11% have been victims of online scams; 10% have been victims of phishing schemes; and 10% have experienced cybercrime on their smartphones. (Norton, 2012)

- 44% of Norton survey respondents were victims of a cybercrime in the previous 12 months, while only 15% reported being victims of an offline crime. (Norton, 2012)

- 35% of adult respondents are fearful of being a victim of cybercrime while online. (Norton, 2012)

- Norton estimates global consumer losses of $388 billion to cybercrime ($114 billion in financial loss and $274 billion worth of their time to deal with the fall out of cybercrime) in 2011 (Norton, 2012)

Online privacy is an ongoing concern for consumers.

- The *2012 U.S. Online and Mobile Privacy Perceptions Report* produced by privacy management solutions provider, TRUSTe shows that:

  - 94% of respondents consider privacy an important issue.

  - 55% of respondents often think about online privacy.

  - 60% are more concerned about their online privacy now than a year ago.

    - 69% say that they trust themselves most when it comes to protecting their own personal information online (up from 45% in 2011).

  - 76% do not allow companies to share their personal information with a third party (up from 67% in 2011).

    - 35% say they have stopped doing business with a company or using their website because of privacy concerns. (RIT, 7/16/2012).

Electronic forms of communication, document sharing and document storage are less secure than their paper counterparts – leading to widespread hacking, data breaches, identity theft and fraud.

- Electronic documents and forms of communication are susceptible to attack by hackers and viruses.

  - In a survey of nearly 600 U.S companies conducted by Ponemon Research, 90% of respondents reported their organizations' computers had been breached by hackers at least once in the previous 12 months." (Ponemon Institute, 2011)

  - Close to 60% of these companies reported more than one breach during the 12- month period. (Ponemon Institute, 2011)

  - Survey respondents cited serious consequences of these attacks: theft of information assets (59%); business disruption (36%); cost of data breach (21%); regulatory and legal action (19%); productivity decline (15%). (Ponemon Institute, 2011)

  - Companies' intellectual property is frequently stored electronically, where it is susceptible to being misplaced or lost through poor data management, stolen by current employees, sabotaged by former employees or stolen by cyberthieves. (McAfee, Inc., 2009)

  - 50% of computer users choose a single common word or keystroke combination for a password that is easy to hack. Hacker software can test for random patterns and break a password code quickly – a 6 letter, lower case password in as little as 10 minutes. (Bloomberg, 2011)

  - Computer viruses can "result in the loss of information and destruction of data." (Harris, 2002)

- Hackers often datamine organization's electronic records for individuals' private information in order to commit fraud.

- For 2012, the following statistics on data breaches for different online segments in the US were reported: 17 data breaches, with 470,048 individual records exposed in the banking/credit/financial sector; 165 breaches, with 4,615,893 records exposed in the business sector; 61 breaches with 2,304,663 records exposed in the education sector; 50 breaches with 7,688,707 records exposed in the government/military sector; 154 breaches with 2,237,873 records exposed in the medical/healthcare sector; for a grand total of 447 data breaches and 17,317,184 records exposed. (ITRC, 2012)

- There were 12.6 million victims of identity fraud in the US in 2012, up more than 1 million from the previous year. Online fraud and data breaches account for the majority of cases. (Javelin, 2013)

- Some types of personal information commonly obtained by data breaches are: credit card numbers, online banking login name and password, and social security numbers. (Javelin, 2013)

- 608,958 cases of consumer fraud were reported to the Consumer Sentinel Network in 2012. Victims of fraud were most frequently targeted electronically (38% through email, 12% via websites or other internet resources) while only 9% of victims were targeted through the mail. (FTC, 2013).

- In addition to targeted hacking, electronic files can be "Google hacked"

  - Search engines and spiders scour the Internet for materials that are then indexed for searching and even archived. "For a variety of reasons -- improperly configured servers, holes in security systems, human error in where an electronic document is stored on a network -- a wide assortment of material not intended to be viewed by the public is, in fact, publicly available. Once Google or another search engine finds it, it is nearly impossible to draw back into secrecy." (Noguchi, 2004)

- Electronic filing of federal tax returns and electronic payment of refunds has led to a skyrocketing number of identity theft tax refund fraud cases.

  - According to the Government Accountability Office, the IRS identified 1,078,000 fraudulent returns in 2012 (642,000 cases plus an additional 436,000 fraudulent returns for citizens of Puerto Rico). It is estimated that 1,500,000 fraudulent returns make it through the system undetected annually. (Novack, 2013).

  - The Consumer Sentinel Network received over 2 million complaints in 2012; the largest single category for 5 years running has been identity theft complaints. 43% of reported identity theft cases involved Federal tax or wage related fraud. (FTC, 2013).

People prefer to receive financial statements and bills in paper format.

- A survey of more than 5,000 US households conducted by Phoenix Marketing International found that:

  - 71% of consumers open print financial statements and bills mailed to them

  - 65% prefer a print copy of their bill or statement

  - about 25% of households don't make electronic payments of any kind

- Identity theft is making people cautious about switching to electronic payments. "The more security breaches there are the more people prefer paper," said PMI President Leon Majors.

- 37% of respondents use mail as their primary method of paying bills. (RIT, January 2012)

- Research on the use of paper by Millennials found that even though 79% of interviewees receive bank statements electronically, 63% print out paper copies of these and other electronic records for their files (TRU, 2011).

- The IRS can audit personal tax returns for up to 3 years and cautions consumers to keep financial records and copies of previous returns for at least that long. Those who bank online may not have access to 3 years worth of previous monthly electronic statements or to images of cancelled checks. (Laise, 2007).

- In a poll of 1,000 registered voters, 72% of respondents want the federal government to continue to issue paper copies of important personal documents, including Social Security checks, annual earning statements and federal tax forms. (Consumers for Paper Options, 2011).

- A survey of UK consumers conducted by Royal Mail revealed that consumers prefer paper banking and billing statements over electronic statements:

    - 73% would feel "inconvenienced and annoyed" if paper statements were discontinued

    - when given a choice, 75% of respondents elect to receive paper statements or a combination of paper and electronic.

    - 65% of respondents who prefer paper statements would consider taking their business elsewhere if a bank or company discontinued the option for print statements (Post & Parcel, 2010)

People trust paper.

- Online interviews with 600 Millennials (TRU, 2011) found:
    - 88% consider paper more official;
    - 82% consider paper more trusted;
    - 78% consider it easier to keep paper confidential;
    - 74% consider paper safer / more secure;
    - 77% believe digital is less trustworthy because it can be altered without your knowledge.

People prefer to keep important documents on paper.

- In a survey of 4,500 European consumers commissioned by Two Sides and Print Power, 63% of 18-24 year old respondents, and 58% of all consumers, prefer to keep important documents on paper. (RIT, 11/2011).

- Online interviews with 600 US Millennials conducted by TRU research revealed that 90% prefer paper copies of important documents (TRU, 2011).

- In a survey of 5,000 consumers conducted by Two Sides, 70% of US respondents prefer to keep important documents on paper. (Two Sides, 2011)

Paper is a stable format with a long shelf life, which makes it ideal for archiving or warehousing information and official documents. Digital storage media, on the other hand, generally have relatively short shelf lives.

- According to a recent survey commissioned by Two Sides, a non-profit organization, 68% of those surveyed believe that paper records are more sustainable than electronic record storage. (RIT, 1/18/2012)

    - In a review of multiple studies on storage media, Lunt provides the following life expectancies for data stored in different digital storage formats: magnetic tape, 10-50 years; magnetic hard disk drives, 1-7 years; flash drives and solid state drives, 10-12 years; recordable optical discs [CD, DVD, Blue Ray], 1-25 years. (Lunt, 2011)

- Certain laws require the keeping of records and documents in print.

    - A number of states in the US and foreign government agencies do not recognize scanned images of a document as an original. (Jedd, 2006)

    - Human resources departments hold on to paper records due to recordkeeping requirements stated by federal employment laws and many state laws. (Thelen, 2009)

SOURCES

Bloomberg Businessweek Magazine (1/27/2011). The Problem with Passwords. http://www.businessweek.com/magazine/content/11_06/b4214036460585.htm

Consumers for Paper Options (9/29/2011). Consumers overwhelmingly support paper options, new poll shows. Press release. http://www.paperoptions.org/links/CPO%20Poll%20Release%209_29.pdf

Federal Trade Commission (FTC) (February 2013). Consumer Sentinel Network data book for January – December 2012. http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf

Gladney, Henry (2007). Preserving digital information. Berlin: Springer-Verlag.

Greenhouse, Steven (3/29/2011). Group seeks labor e-mails by Michigan professors. *The New* York Times. http://www.nytimes.com/2011/03/30/education/30professors.html?_r=0

Harris, Micalyn S. (2002). Is email privacy an oxymoron? Meeting the challenge of formulating a company email policy. *Journal of Civil Rights and Economic Development* 16(3): 553-567. http://scholarship.law.stjohns.edu/jcred/vol16/iss3/2

Identity Theft Resource Center [ITRC] (12/26/2012). 2012 Data breach stats. http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202012.pdf

Javelin Strategy & Research (2/20/2013). More than 12 million identity fraud victims in 2012 according to latest javelin strategy & research. Reporthttps://www.javelinstrategy.com/news/1387/92/More-Than-12-Million-Identity-Fraud-Victims-in-2012-According-to-Latest-Javelin-Strategy-Research-Report/d,pressRoomDetail

Jedd, Marcia (2006). Don't forget the paper. *AIIM E-DOC* 20(3): 42-45.

Laise, Eleanor (2007). Pushing paperless: The pros and cons. *The Wall Street Journal* May 2, 2007.

Lunt, Barry M. (2011). How long is long-term data storage? *Archiving 2011 Final Program and Proceedings*, p. 29-33. http://www.imaging.org/ist/publications/reporter/articles/REP26_3_4_ARCH2011_Lunt.pdf

McAfee, Inc. (2009). Unsecured economies: Protecting vital information. http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf

Noguchi, Yuki (2/9/2004). Online search engines help lift cover of privacy. *Washington Post* Page A01. http://jrichardstevens.com/articles/noguchi-searchprivacy.pdf

Norton. (2012). Norton cybercrime report 2011. http://us.norton.com/cybercrimereport/promo

Novack, Janet (1/29/2013). IRS tips won't protect you from identity theft tax fraud. *Forbes*. http://www.forbes.com/sites/janetnovack/2013/01/29/irs-tips-wont-protect-you-from-identity-theft-tax-fraud/

Post & Parcel (9/16/2010). Study highlights importance of paper statements. *Post & Parcel*. http://postandparcel.info/34696/in-depth/study-highlights-importance-of-paper-statements/

Ponemon Institute (June 2011). Perceptions about network security. Survey of IT & IT security practitioners in the U.S. http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf

RIT (7/16/2012). 94% of consumers say online privacy is important to them. *Print in the Mix*. http://printinthemix.com/Fastfacts/Show/587

RIT (1/18/2012). Americans still prefer print and paper communications. *Print in the Mix*. http://printinthemix.com/fastfacts/show/519

RIT (January 2012). Print statements and bills still favored by many U.S. consumers. *Print in the Mix*. http://printinthemix.com/fastfacts/show/592

RIT (11/2011). Electronic media vs. print: All generations prefer paper. *Print in the Mix*. http://printinthemix.com/Fastfacts/Show/513

Ross, Seamus (2012). Digital preservation, archival science and methodological foundations for digital libraries. *New review of information networking* 17(1): 43-68.

Thelen, James B. (2009). On and off the paperless trail. *HR Magazine* 54(3): 75-77.

TRU research (2011). *Millennial paper usage and attitudes*. Paper presented at Paper2011, sponsored by the American Forest & Paper Assn and the National Paper Trade Alliance, March 2011.

Two Sides (9/2011). Consumers' environmental perceptions of print & paper.