IMRA: ISM Provisions

Data retention: Legal obligations and technical challenges
Presentation by Jeff Sybesma

My presentation will be structured as follows. I will start with some general remarks. Then I will elaborate on three questions, namely What do we store, Why do we store and How do we store. I will close with some conclusions.

I. General remarks

The topic of my presentation is Data Retention. So the first question to be answered is: What is data? The term data refers to qualitative or quantitative attributes of a variable or set of variables. Data (plural of "datum") are typically the results of measurements and can be the basis of graphs, images, or observations or a set of variables. Data are often viewed as the lowest level of abstraction from which information and then knowledge are derived.

Raw data, i.e. unprocessed data, refers to a collection of numbers, characters, images or other outputs from devices that collect information to convert physical quantities into symbols.

Also, data is a representation of a fact, figure, and idea. Such usage is the origin of data as a concept in computer science: data are numbers, words, images, etc., accepted as they stand.

The terms information and knowledge are frequently used for overlapping concepts. The main difference is in the level of abstraction being considered. Data is the lowest level of abstraction, information is the next level, and finally, knowledge is the highest level among all three.

Data on its own carries no meaning. For data to become information, it must be interpreted and take on a meaning. For example, the height of Mount Everest is generally considered as "data". A book on Mt. Everest geological characteristics may be considered as "information", and a report containing practical information on the best way to reach Mount Everest's peak may be considered as "knowledge".

In computing, data is information that has been translated into a form that is more convenient to move or process. Relative to today's computers and transmission media, data is information converted into binary digital form.

What is data retention? Data retention defines the policies of persistent data and records management for meeting legal and business data archival requirements. A data retention policy weighs legal and privacy concerns against economics and need to know concerns to determine the retention time, archival rules, data formats, and the permissible means of storage, access, and encryption.

II. What do we store?

Data is increasing on a daily basis. Our digital universe keeps expanding!

Let me give an example. I am a fanatic digital photographer. Many people ask me how much pixels my camera is capable of capturing. When I say 18 megapixels everyone is impressed. But this also means that every picture that is captured will need some 20 MB of disk space. If you shoot in Raw and transform this to a Jpeg picture, then the memory space needed will doubled. Can you imagine that I have a TerraByte of hard disk space in my computer, and I am still struggling for more disk space!

- The projected growth of the digital universe could outpace our ability to manage it, creating new challenges and opportunities.
- Every time we backup a report or send an e-mail, take a digital photo, blog, upload a video or download a song, we are contributing digital content.
- In 2009, the digital universe grew by a staggering 62% to about 800,000 petabytes (a million gigabytes).
- In 2010, the digital universe was expected to grow to 1.2 million petabytes and will reach 35 trillion gigabytes by 2020. That would fill a stack of DVDs that would reach half way to Mars.
- Over the course of the next 20 years, the digital universe will grow by 44 times.
- Issues that arise include the amount of physical storage needed to contain all this data. This is in part attributable to the fact that only 25% of digital content being created is unique – the other 75% consists of things such as forwarded e-mails and other copies.

Therefore originals are important to keep and not copies!

- In a world filled with computer printers, fax machines, photocopiers and scanners, the notion of an "original" is somewhat slippery. It is more common to refer to the "authoritative" or "master" copy of a record that is designated as the official data source.
- Electronic copies of records originally on paper may be acceptable as a substitute.
  - However, retention of the original paper may be required as an authoritative source.
- Conversely, printouts of electronic files may be considered acceptable substitutes.

- It is up to the organization to assure that appropriate retention occurs for all the data for which they are responsible.
- Finding what we need in all this data will require continued advances in ways to manage it. That includes ways to know when to delete data, and search tools to find what we need.
- The amount of data that needs protection will increase at even a faster rate. This includes confidential and personal information, such as financial and health data.
    - Less than 10% of the information about an individual is created by the individual himself – such as taking photos, using social media, sending e-mails, and getting cash from an ATM.
    - The rest is created by others, such as credit records, surveillance photos and web-use histories.
- Managing the security and privacy of all this will continue to be a challenge.

Why do we retain all this data? Is it necessary? In my personal case with the thousands of pictures that I have retained as digital data the reason is primarily emotional: it shows my creative and personal products as a photographer. But how about all data created in a working environment? In this case there are external and internal obligations to retain data.

The external needs

- legal-regulatory requirements
    - tax laws
    - general auditing requirements
    - supervisory requirements
- standards of private certificatory bodies
    - e.g. ISO norms
- contractual obligations to other parties

The internal needs

- information needs of the organization

III. Why do we store?

This brings us to a next question of my presentation, namely the question 'why do we store data'. First the law.

Book 2 of the Civil Code of Curaçao states in article 15 the following:

1. The management must, for administrative purposes, keep a record of the financial condition and of everything relating to the activities of the legal person according to the requirements to which such activities give rise, and it must keep the books, documents and other data-carriers in respect thereof in such manner that the rights and obligations of the legal person can be ascertained therefore at any time.

2. Without prejudice to the provisions elsewhere in the law, the management must annually, within eight month from the end of the financial year, prepare a written annual account, comprising at least a balance sheet and a statement of income and expenditure.
3. The management must keep the books, documents and other data-carriers referred to in paragraphs 1 and 2 for ten years.
4. All data recorded on a data-carrier, except for the written balance sheet and statement of income and expenditure, may be transmitted to and kept on any other data-carrier, provided the data are rendered correctly and completely when such transmission is made and these will be available during the entire period these must be kept and can be rendered legible within a reasonable time.

A legal person can be, according to article 1 paragraph 1 of Book 2 Civil Code of Curaçao, the foundation (Stichting), the private foundation (SPF), the association (Vereniging), the co-operative (Coöperatie), the mutual insurance society (Onderlinge waarborgmaatschappij), the public limited liability company (NV) and the private limited liability company (BV).

Interesting detail is laid down in paragraph 2 of article 1 of Book 2, where it states that the articles of the general chapter (including the previous mentioned article 15) may be applied mutatis mutandis to such other legal entities, except to the extent where this would be contrary to the law and the nature of such legal person. An example of such a legal entity is the Central Bank of Curaçao and Sint Maarten; or SVB or APNA. Also the country Curaçao is a legal entity.

Other legal obligations to keep relevant data for at least ten (10) years can be found in supervision legislation. For example, the National Ordinance on supervision of credit institutions (LTBK PB 1994, No. 4) explicitly states in article 42 that credit institutions are obliged to keep for at least ten (10) years all letters, supporting documents and other data carriers (media) with regard to the institution and also all records regarding mutations on personal and other persons accounts with accompanying letters, supporting documents and data carriers (media).

The Central Bank's Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing for Credit Institutions (2011) also have a chapter on record keeping.

Record keeping: All necessary records on transactions (both domestic and international) must be maintained for at least five years after the transaction took place. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts, currencies, and type of transaction involved) so as to provide, if necessary, evidence for prosecution of criminal behavior.
Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business

correspondence must be kept for at least five years after the business relationship has been discontinued.

And the Central Bank's Provisions and Guidelines for Safe and Sound Electronic Banking (2011) states:

Recordkeeping: All e-banking transactions should generate clear audit trails, which should be archived and kept for 10 years. ATM video surveillance recordings should be archived for at least one year. It is also vital to generate and protect records of customer instructions in a legally acceptable format. Credit institutions should strengthen information security controls to preserve the confidentiality and integrity of customer data. Firewalls, ethical hacking tests, physical and logical access controls are some of the methods available. Recordkeeping requirements should be based upon the level of activity and risk.

IV. How do we store?

If we are obliged to store and retain data, the next question is **how** do we store?
Keep in mind that data is not only digital

Managing **physical** records

- Identifying records
    - a legal record, it needs to be authenticated
- Storing records
    - accessible
        - data protection
    - safeguarded against environmental damage
        - filing cabinet, safe or vault
    - safeguarding against unauthorized access
        - Privacy and identity theft
- Circulating records
    - Tracking Systems
        - Electronic Document and Records Management Systems (EDRMS).
- Disposal of records
    - Archiving (short term or long term)
    - shredding

Managing **electronic** records
The general principles of records management apply to records in any format.
Digital records (almost always referred to as electronic records) raise specific issues. It is more difficult to ensure that the content, the context and the structure of records is preserved and protected when the records do not have a physical existence.

Digital preservation: the ability to access and read electronic records over time, since the rapid pace of change in technology can make the software and hardware used to create and store the records obsolete, leaving the records unreadable.

Storage media
Bulk data storage, backup, archiving, and interchange

- Magnetic tape
    - has been used for this purpose for decades

- Hard disk
    - capacity/price ratio improved rapidly



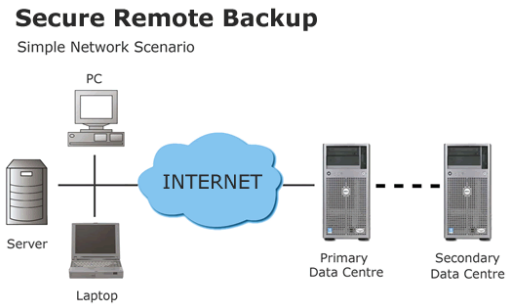
- Optical storage
    - CD, DVD, Blu-ray Discs


- Floppy disk

8 inch, 5,25 inch, 3,50 inch

- Solid state storage
    - flash memory, thumb drives, USB flash drives, CompactFlash, SmartMedia, Memory Stick, Secure Digital cards, etc.

- Remote backup service
    - Via broadband internet access to remote location
        - Trust of a third party service provider



So, we backup data. The question is how?

Data repository models

Any backup strategy starts with a concept of a data repository. The backup data needs to be stored somehow and probably should be organized to some degree.

- Unstructured
- Full + incremental
- Differential backup
- Reverse delta
- Continuous data protection
- Full system backup

Which system to use? Every organization, big or small, needs to think through and decide what data retention strategy must be put in place with respects to organizations needs, obligations and possibilities.

Again, I would like to give you my own personal experience as a photographer with regard to making backups. My, and I believe everybody's biggest nightmare is always a crash of your hard disk! Thousands of my precious pictures lost. Memories lost! And no possibility to remake them. So to mitigate this risk I installed two 500 GB hard disks into my PC and made it a costume to save every picture on both disks. In case of a crash the other hard disk still gives access to all my pictures. In doing so I thought I have in place a reliable backup system. Until my whole PC was stolen during a robbery at my house.

V. Conclusions

With regard to data retention an organization needs to address many questions:

1. What data must be held?
2. Where must that data be held.
3. How long must the data be held.
4. How must the data be handled when a legal hold is received and maintained during an investigation or lawsuit.

The organization faces:

- Legal challenges
  - By law or contract
  - Retention minimums vs. maximums?

    Minimum time of retention
    - External data retention requirements are usually set as minimums
    - Organizations may in most circumstances elect longer periods at their discretion

    Maximum time of retention
    - Confidentiality interests of the data subject
      - criminal and integrity records
    - Storage and security costs

- Technical challenges
  - Hard- and software
  - Specific internal needs

To end my presentation I would like to read from an article by Kevin Beaver, an American independent Information Security Consultant.

The title of his article is: A thorough data retention strategy needs more than just IT oversight

He states that … Based on what I see when performing security assessments, litigation support and expert witness work, there's hardly anything posing as much of a threat to businesses today as the mismanagement of data retention. Simply put, a data retention strategy is often handled as any other function of IT -- but it just doesn't work that way.

As with most things that affect the bottom line -- supply chain management, finance, sales, etc. -- there has to be some level of accountability through checks and balances across the board. In areas such as those just mentioned, that's usually the case. However, there's often little to no oversight when it comes to data retention requirements. This goes for corporations, nonprofits and government agencies of all sizes.

In certain cases where a data retention program does exist, it’s often in the form of a data retention policy that’s been haphazardly thrown together. Data retention strategies such as these don’t implement what’s needed or, worse, are downloaded off the Internet without any real tweaking based on the business’s data retention requirements and specific circumstances.

A thorough data retention strategy needs to involve the legal department, internal audits, human resources and executive management.

Whether it’s to satisfy an internal policy, business partner requirement, external audit or legal hold for e-discovery, data retention strategy is a serious business issue that deserves serious attention from the proper stakeholders.

By not addressing these issues now -- before you need to -- you risk unnecessary liabilities by having too much data lying around, as well as spoliation (plundering) or other mishandling that can really get your business in hot water.

Unless you have people outside IT helping to call the shots on data retention requirements, it's a huge risk right under your nose -- and one the IT department will never be able to handle independently.

Thank you for your attention