Electronic Document Handling in the Armed Forces : Need for an Automated Approach

Commander K Ashok Menon (Retd)*

Background

The instances of leakage of Radia Tapes, the draft version of the Coal Block allocation issued by Comptroller and Auditor General (CAG) getting to the public domain, the Chief of Army Staff's classified communication to the Defence Minister reaching the press and last but not the least, Defence Research Development Organisation's (DRDO) inability to fathom leakage of an internal audit report, against all laid down norms, are some of the instances in the recent past where the agencies concerned are having their backs against the wall and grappling to find a way to contain this menace. The thin line that separates 'information theft' from 'information leakage' is indeed hard to define and perhaps has to be inferred on the basis of the context. That such action, malafide or otherwise would happen in any era is natural to assume, but the ease with which it can be done today, is a matter of concern that needs urgent addressing.

The Economist in its Feb 2011 edition[1] had stated "They are one reason why International Data Corporation (IDC), a market-research firm, predicts that the "digital universe", the amount of digital information created and replicated in a year, will increase to 35 zettabytes by 2020, from less than 1 zettabyte in 2009; 1 zettabyte is 1 trillion gigabytes, or the equivalent of 250 billion DVDs. But these tools will also make a firm's borders ever more porous. "WikiLeaks is just a reflection of the problem that more and more data are produced and can leak out," says John Mancini, president of Association for Information and Image Management (AIIM), an organisation dedicated to improving information management". An earlier IDC paper[2] had deduced that an average

***Commander K Ashok Menon (Retd)** comes from a core technology background. He holds a Master's degree in Mathematics, Operations Research and Software Systems. During his career spanning 27 years, he was involved in varied fields of Information Technology and Consultancy Systems. Currently, he is Managing Director Periculum Technology and Consultancy Systems.

Journal of the United Service Institution of India, Vol. CXLI, No. 589, July-September 2012.

1 MB file attachment has a footprint, 50 times as large within the organisation's intranet. Whether, in the first place such a large circulation of copies of a document is needed, is one debate, but importantly after it reaches the respective recipient, how long should it 'exist' is another. Even greater is the debate on how an enforcement of the 'cradle to grave' principle can be achieved.

E-Document and the Armed Forces

The electronic document editors; be it Word Processor, Spread Sheet or Presentation packages in the form of MS Word, MS Excel and MS PowerPoint deployed across the Forces have empowered users at all levels to templatise, crunch data or facilitate authoring presentations effectively. This has undoubtedly become a high-end productive tool set whose efficiencies are not measured normally as it is taken as a base-line for day to day functioning. With the proliferation of the number of Personal Computers across units, formations, ships and establishments, each pre-loaded with an MS Office package, an end user leverages the same to see that files of the various formats stated above are stored on the respective machine. Customarily, these machines are on a centralised Network, in few cases, Local Area Networks of different sizes. There are machines that operate on a stand-alone mode too.

Navy, for example, with its New Energy Systems Group (NEWN) backbone has been able to ensure that a most of the Local Area Networks that were hitherto operating in isolation are integrated with it. It is therefore imminent that, gradually a complete centralised control would come about. Across the three services there have been a few ERP implementations apart from Messaging solutions, that have matured during the 1990's. Again in the case of the Navy, one of the successful implementations over NEWN has been the Navy wide E-Mail solution - it has been in operation for a few years now. There are also a few structured Enterprise Resource Planning (ERP)/ centralised implementations that are used by a defined set of users, like Messaging/Communication, COTS ERP for Sailors, home grown ERP for General and Aviation Logistics etc. Similar centralised messaging solutions and applications for Ordnance and Inventory do exist in the other two services. In all such cases, however, control of access to information is implemented through the respective solution framework itself. Responsibility and ownership of ensuring the same also, lie within the specific application's administration group. Further, in most of these cases it is relatively easy to audit and check effectiveness of how these controls are implemented, because of the nature of the architecture and tools used.

Since the number of such ERP or centralised applications – are very few, it is evident that maximum amount of information on an on-going basis is generated on workstations, through a combination of Office utilities like a Word Processor or a Spread Sheet. It would also be fair to assume that such information, which could be of varied degrees of criticality and importance, is made available to the entire senior leadership, leveraging standard packages like MS Office. It is relevant to mention that while there would be a few implementations of Office Packages on other Operating Systems, like Linux for example, a substantial percentage of users use MS Office on Microsoft Windows.

Currently, as a practice, each user classifies a document, by typing an appropriate classification label, say 'Secret' or 'Confidential' on the top and bottom of each page. As a policy, 'Secret' and above classified documents are not to be held in electronic form, and the permitted classified documents are to be stored only in encrypted form.

Periodic Information Security audits, are undertaken to check and confirm effectiveness of IT Security issues in various directorates/units.

Concerns

Against the above backdrop, following are some of the concerns that are likely to exist:-

(a) Lack of a 100 per cent integrated IT infrastructure, that allows information assets to be created and held in islands.

(b) Data created on a day to day basis, over a period of time builds the information inventory on each workstation, with no mechanism available to know the nature of content that each machine holds.

(c) Due to lack of any form of automation, there is nil visibility of a establishment's/unit's/directorate's - Document-Inventory holding.

(d) As a corollary there is nil visibility on the amount of classified information held on each machine / across the Organisation - in absolute terms.

(e) Resultantly when an IT asset (workstation, hard-disk, laptop etc.) is lost, the Organisation has no visibility on the quantum of classified information lost.

(f) While encryption tools have been installed on each machine for encrypting local documents held, there is no mechanism to establish whether it is actually used, unless a physical check on each machine is carried out. This implies significant possibility of:-

(i) Presence of un-encrypted 'confidential' documents in a workstation

(ii) Presence of un-encrypted documents labeled 'Secret' or 'Top Secret' in a workstation.

(g) Since noting sheets, memos etc. are all typed in MS Word and further since important justifications are given by embedding data from MS Excel Files into these Word documents, it is apparent that condensed critical and confidential information is likely to be lying strewn in various workstations across the enterprise and in many cases unencrypted.

(h) Lack of an automated audit measurement tool to check classified information held, aggravates this risk dimension further.

(j) With increase in usage of internal e-mail, it would be fair to assume that 'attachments' containing critical information are held in multiple workstations. This apart from creating overheads in storage, importantly increases risk exposure due to leakage from multiple sources.[3]

Key Information Security Lessons from WikiLeaks

A cursory glance at the Wikileaks site reveals that, content obtained by the Wikileaks owners was pushed by them into a structured Database from which retrieval was simple. Information was organised based on 'location' and 'classification-label'. A quantified statistic in terms of classified content held was most certainly a powerful representation of the likely loss to the stake-holder, reputational or otherwise.[4]

The key question here however is whether the concerned stakeholder itself - say a specific embassy in this case - have details of the content it would have lost – and more importantly, held it in a similar fashion, as presented by the Wikileaks site. If indeed had the information in such granular detail been available to any tier of leadership within, perhaps the mechanism that would have been in place to protect it, would have been different.

Recommended Approach for Complete Document Protection

While there are tools in Document Management, Information Rights Management etc., the complexity of the Services Organisation makes it difficult to implement these even if the IT maturity within the set-up goes up substantially. However, there is a compelling case to address e-Document protection.

It is clear from the facts brought out that in order to protect Electronic Documentation created through utilities like MS Office that draw strength from its de-centralised architecture, deployed across multiple workstations, in a fragmented network environment, a tailored approach that leverages innovative use of technology combined with effective management processes needs to come into play.

Following are the recommended steps to attain the objective of achieving a reasonable assurance on document protection:-

(a) Build an Information Security culture that sensitises the importance of each individual's role in the Document Creation and Management Process.

(b) Make aware the criticality of the A 7.2 control of the ISO 27001 standard on Information Security that deals with Data Classification to all personnel.

(c) Take steps to incrementally build localised databases of classified content held within a workstation, across units/ ships/directorates.

(d) Take steps to create a centralised repository that integrates information stored in these localised databases. This repository acts as the basic audit database that provides:-

(i) Summarised information on overall document holding of the enterprise.

(ii) Summarised information of classified documents held across the enterprise.

(iii) Drill down details for audit and basic forensic purposes.

These steps are possible only with deployment of an automated tool to enforce classification of documents. Any other alternative, like maintenance of manual register - introduces subjectivity. Also physical verification for audit would be a non-starter. The choice of tool should ensure following:-

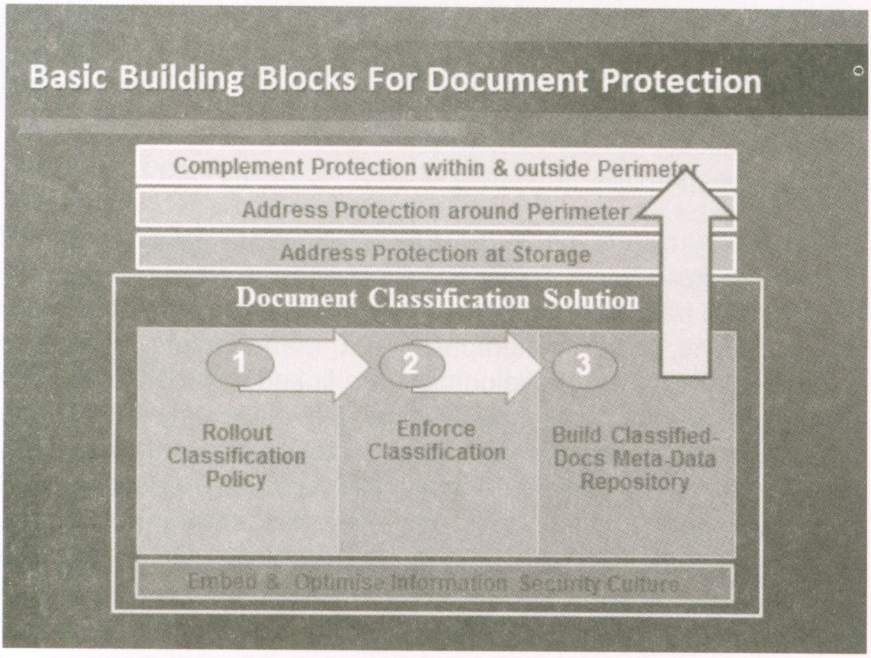
(a) It should integrate with the encryption tool that is currently in use for end point document encryption.

(b) It should enhance the effectiveness of encryption usage.

(c) It should be possible to implement a suitable Data Leakage Prevention solution that integrates with the Document Classification Solution. This solution would ensure that logs are created when classified documents are being 'sent' or 'copied'. Adequate controls around despatch of information can also be built. Essentially this would address content leaving the perimeter of the organisation.

Once the above is completed, a more informed decision on whether and how document flow within the environment needs to be controlled, can be taken. Based on the same, an appropriate Information Rights Management tool could be deployed, in a phased and defined manner – where relevant. The reason why this point is being emphasised, is because of the highly rule-driven nature of the tool sets available. This would have an impact on its successful implementation across the Organisation – because of the complex dynamics of the environment.

Based on the facts stated above, a layered approach to protect e-documents is recommended. Diagrammatic representation of the same is shown at **Figure 1.**



Basic Building Blocks For Document Protection

Complement Protection within & outside Perimeter

Address Protection around Perimeter

Address Protection at Storage

Document Classification Solution

1 Rollout Classification Policy

2 Enforce Classification

3 Build Classified-Docs Meta-Data Repository

Embed & Optimise Information Security Culture

Figure 1

Conclusion

The proliferation of electronic documents within the Armed Forces on the one hand and the complexity and challenges associated with augmenting IT assets with sustained rapidity has begun to throw up the inadequacies in addressing electronic document handling. Digital Forensics is used for investigation purposes currently and would continue–but this is after an Information Security incident has occurred.

With leakages of data/documents taking place at periodic intervals, there is a compelling need to be proactive. That can happen only if the basic aspect of creating visibility of the e-Document Inventory – which also acts as an audit database - is addressed with speed.

Endnotes

1. Companies and information/ The leaky corporation – The Economist – 24 Feb 2011.

2. The Diverse and Exploding Digital Universe – An IDC White Paper sponsored by EMC – March 2008.

3. The Diverse and Exploding Digital Universe – An IDC White Paper sponsored by EMC – March 2008.