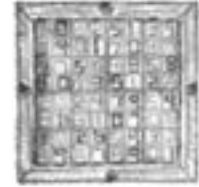


OFFICE CONTENT MANAGEMENT SECURITY

CHUCK NETTLESHIP, *Cipher Systems*



As CI professionals, we gather vast amounts of sensitive information, we compile it into meaningful reports, and then we communicate the results to those who need it. We take great care to secure internal *front-end* information through network firewalls, encryption, and redundant information technology systems to prevent viruses, network intrusion, and access to company proprietary information.

But what happens when we are done with our old paper files, computers, and cell phones? Unfortunately, many organizations do not actively monitor and conduct life cycle risk assessments for *end-of-use* electronic assets and paper data.

In an earlier column we covered several important points on keeping data and networks secure, but what about data storage devices and office paper that is discarded or simply disappears at end of use? Here are a few ideas to consider for life-cycle asset management of obsolete data and electronics, coupled with environmental practices to protect against the vulnerabilities of data loss within an organization. This column will focus on common-sense steps to integrate in an existing process or establish a new one.

STEP 1: DUE DILIGENCE

Performing a due diligence internal audit of current information life-cycle management practices will pay dividends for any organization – public or private. You need to know where the holes and the susceptible points of access are, then fix them. This is the only way to prevent the loss of proprietary information, reduce the risk of client lawsuits, and mitigate the

chance of possible prosecution under local, state, federal, or international law.

As an important first step, recognize all of the sources where data may reside within your department or organization. As information professionals, we are responsible for tangible physical paper-based data and intangible bytes of information hidden within the virtual world of mobile phones, personal data organizer memory chips, and computer and server hard drives.

Consider this 2002 incident. With the best of intentions, the Department of Veterans Affairs donated over 100 computers to educational institutions. But the process was flawed: they did not completely erase all sensitive information from the hard drives prior to donation. In response, the agency established and institutionalized information life-cycle best practices, including an electronic audit, a comprehensive risk assessment, and erasing data storage devices to Department of Defense DoD 5220.22-M (triple-wipe) standards. Information security officers and staff now receive relevant training and purchased software to erase hard drives prior to donation or disposition.

Physical data resides in paper-based reports, financial data, memos, handwritten notes, mail envelopes (return addresses), and a wide variety of other items in an office environment. Electronic content can be found not only in the more obvious places – databases, data files, emails, websites, and blogs – but also embedded in removable hardware devices like internal or external hard-drives, personal digital assistants (PDAs), subscriber identity module (SIM) cards, and flash drives. When

obsolete, these items may be donated to schools, resold, placed in the garbage, recycled, or managed through outsourced vendors. All end-of-life disposal options need to be taken into consideration when a particular dataset or device becomes aged and timed for deletion.

STEP 2: AWARENESS

Given the various types of data sources, you should consider two key avenues and areas of potential vulnerability when planning for the disposal of information and electronics: environmental and technological. You need to build awareness in both areas.

From the environmental standpoint, we have witnessed many corporations implementing ISO 9001/1400 recycling programs and office waste reduction strategies. Recycling is important (and in some jurisdictions mandatory), but you need to take great care in deciding what to recycle, how it is done, and which vendor to select.

From the technological standpoint, data files may be deleted, but remember that hidden files on an unsuspected C-drive or a confidential project on a CD-ROM may be left in a donated or resold personal computer, or a hard drive may simply slip through internal or subcontracted information technology processes if not managed or tracked carefully.

ENVIRONMENTAL AWARENESS

Office recycling programs often use local recycling centers or contract with local recycling service vendors. This leaves several open access points to potentially sensitive information if the

SIDEBAR 1: STEPS TO GUIDE IN THE AUDIT PROCESS

- Integrate environmental and electronic best practices into business planning.
- Evaluate your existing in-house or outsourced electronic management infrastructure.
- Involve procurement and information technology and management departments to collaborate and develop purchasing and disposal strategies that meet both the needs of the entire organization and regulatory compliance requirements.
- Review the best options for electronic management: lease vs. purchase.
- Review end-of-life options and budget accordingly: donation vs. recycling vs. destruction.
- Conduct an internal audit of current and future electronic assets, data storage, and solid waste. This can be outsourced to a professional waste management professional, or consultant, or accomplished through internal resources.
- Have end-of-life electronics disposition vendors (recyclers) provide certifications of data destruction or *triple wipe* of hard drives if resold.
- Audit the vendor's procedures and have them provide an audit trail of their process for disposition of electronics, office paper, and other recyclables.
- Visit the vendor's facility and walk through their disposition process.
- Ensure that the recyclables do not end up in a landfill if you are paying for full-service disposal.
- Make sure that there is an audit trail of where your material ends up (percent of material recycled, sent to landfill, overseas sales, re-sale).
- Conduct periodic internal and external vendor reviews.

documents or devices being recycled are not appropriately shredded or destroyed prior to delivery. Although this information may no longer be of use internally, this garbage may be sold to someone else, particularly competitors. Whether the material is going into a recycle bin or a garbage can, make sure that you are cognizant of what you may be sharing if you do not properly destroy it first.

Many recycling and disposal vendors advertise closed-loop processes that suggest your recycled materials will be used for new product. All too often these same vendors actually dispose of your materials in landfills or barges overseas. While some items are justified for landfills if no cost-effective recycling end-market exists, you should close the loop yourself and demand to see their process. If they aren't forthcoming with details, they may be trying to hide something from you.

Some electronic waste contains harmful material like lead and other Environmental Protection Agency (EPA) regulated materials that make safe disposal an even greater challenge. States regulate waste differently, so check with local and state solid waste regulators to ensure that your solid waste management plan and vendor are in compliance with applicable laws and regulations.

TECHNOLOGICAL AWARENESS

Several commonly used electronic items may retain data after back-up; sometimes simply deleting files is not enough. In addition, people often maintain copies of files in multiple places. Control and accountability of these points of access should be documented and communicated. Disposal processes of the following need to be carefully considered.

Tangibles:

- Office paper, contracts, old files and mail – shred material in-house or outsource to a reliable vendor

Intangible data inside tangible electronics:

- computers: hard drives and check for CD's left in the computer
- servers: hard drives and memory tapes
- external data storage devices
- copy/fax machines: many new machines have hard drives that retain data
- PDAs and external storage devices: memory chips with personal information, corporate contact lists, credit card information and pass codes, personal identification numbers (PINS)
- mobile phones: memory chips, SIM cards
- digital cameras: memory chips, SIM cards, digital photographs
- memory "sticks"
- global positioning systems (GPS) devices and hand-held radios (frequencies, crystals)

STEP 3: REGULATORY COMPLIANCE

While developing your end-of-life/end-of-use information security strategy, be aware of the many laws and acts surrounding data retention and protection. Remember that regulations for Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley require that information be protected at all times. Part of the Sarbanes-Oxley Act states that anyone who knowingly destroys documents or files that may relate to a federal investigation or a bankruptcy filing can be imprisoned for up to 20 years.

Obtain a briefing from your corporate counsel on your responsibilities for safeguarding records in the event of a lawsuit, federal investigation, or bankruptcy. A document management company may be able to assist with internal organization and knowledge management of material. Digitize (scan) data to reduce paper, provide

ease of retrieval, and manage corporate knowledge.

Destroy the data on disk drives and similar electronic media using processes compliant with DoD 5220.22-M and private sector standards. Several software vendors and local and national electronic life-cycle management companies provide compliant data destruction services.

Several regulatory issues surround waste management. These all need to be taken into consideration, particularly when it comes to recycling and disposal processes. Consult your local and state departments of solid waste and recycling offices for current laws and regulations. The EPA can also provide additional guidance.

STEP 4: IMPLEMENT A STRUCTURED PROCESS

Simultaneously audit and integrate environmental and electronic management best practices. This allows managers to monitor vulnerabilities, review current procedures, and evaluate data management procedures.

Use internal staff, outsource, or use a combination of both internal and external professionals to develop a systematic approach for retiring and managing obsolete electronic equipment and waste office paper. Look at the options best suited for your department or organization,

consult current vendors, or research other vendors that fit your specific needs and look to future technology trends that provide overall network and end-of-life data protection. Sidebar 1 shows a few steps to guide the auditing process.

The basic principles considered here are rooted in common sense. However, without a thorough and periodic risk assessment or audit, organizations leave themselves and their clients vulnerable to loss of data through unsuspected means. Follow these simple suggestions to protect obsolete end-of-life electronics, office paper, and other potential data-containing materials from the eyes of competitors and identity thieves.

RESOURCE LINKS

The links below are to industry trade organizations that offer additional resources, strategies, and information about electronic recycling, office recycling, and solid waste management options. Contact your state and local recycling offices for compliance details.

Electronics

Electronics Industry Alliance (www.eia.org)

International Alliance of Electronics Recyclers (www.iaer.org)

General

American Forest and Paper Institute (www.afandpa.org)

American Iron and Steel Institute (www.steel.org)

American Plastics Council (www.americanplasticscouncil.org)

Institute of Scrap Recycling Industries (www.isri.org)

National Recycling Coalition (www.nrc-recycle.org)

Polystyrene Packaging Council (www.polystyrene.org)

Steel Recycling Institute (www.recycle-steel.org)

Vinyl Institute (www.vinylinfo.org)

Chuck Nettleship is the director of intelligence solutions at Cipher Systems (www.cipher-sys.com). He worked for several years developing solid waste and recycling audit and best practice strategies for local, state, and federal agencies and private corporations. Most recently, Chuck was in Iraq and was involved with force protection and media exploitation. Cipher specializes in competitive intelligence consulting, document management, and technology services for both the public and private sectors. Services include primary and secondary data collection, analysis, reporting, company profiling and scenario planning. Chuck can be reached at c.nettleship@cipher-sys.com or 01.410.451.6889.

SCIP06 • April 26-29 • Orlando, FL

The: SCIP Best Practice Forum: ROI and CI is a "must-attend" event for all CI professionals interested in demonstrating and measuring the value of CI. This is your opportunity to benchmark your CI efforts. Plus, attend the Best Practice Forum and you will receive and participate in:

- Access to an award-winning "progressive case study";

- Best practice sharing session conducted by a professional facilitator;
- An interactive, hands-on experience with seasoned CI professionals;
- A great networking reception to keep you connected with your fellow attendees;

- Comprehensive program materials as well as breakfast, lunch and refreshments each day

The SCIP Best Practice Forum is valuable to your success as a CI professional. The SCIP conference hotel reduced rate is only available until February 20, 2006. Full details at www.scip.org