

## Protecting the environment, your data and your budget.

In today's climate, we all have a duty of care to sustain global resources. However this should not be at the cost of your ability to protect business critical data, control business IT assets or manage your budget.

Myles Pilkington  
10/11 November, 2009  
Green IT Expo

# Agenda

- Protecting the Environment
- Protecting your Data
- Protecting your Budget



# Protecting the environment

**Introduction**

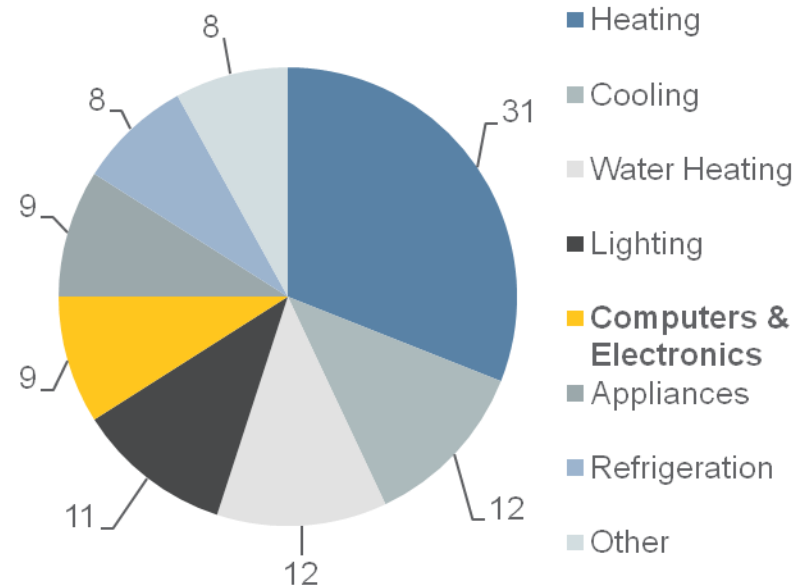
# IT and Sustainability

- Definition of Sustainability
  - World Commission on Environment and Development - "[to meet] the needs of the present without compromising the ability of future generations to meet their own needs."
- Quest for Sustainability
  - Centre for Sustainability - "The same business practices that improve social and environmental capital have been shown to also improve long-term profitability. When implemented, sustainable business practices provide an avenue to achieve mutual benefits in the natural world, the community, and the economy."

# “Dirty IT” and the Environment

- IT uses energy / pollutes
  - 9% of US power usage and rising
- IT uses precious resources
  - 1.8 tonnes of resource required to manufacture 1 desktop station
- IT is hazardous
  - New legislation is addressing, but current equipment uses lead, phosphors, cadmium, etc.
- IT impact is growing
  - In 2008, 1 billion PCs in use globally (after 27 years of use)
  - By 2015, 2 billion PCs will be in use
- IT resource is being lost
  - End of 2007, an estimated 2 billion PCs had been manufactured  
**(what happened to the other billion?)**

## US Power Usage

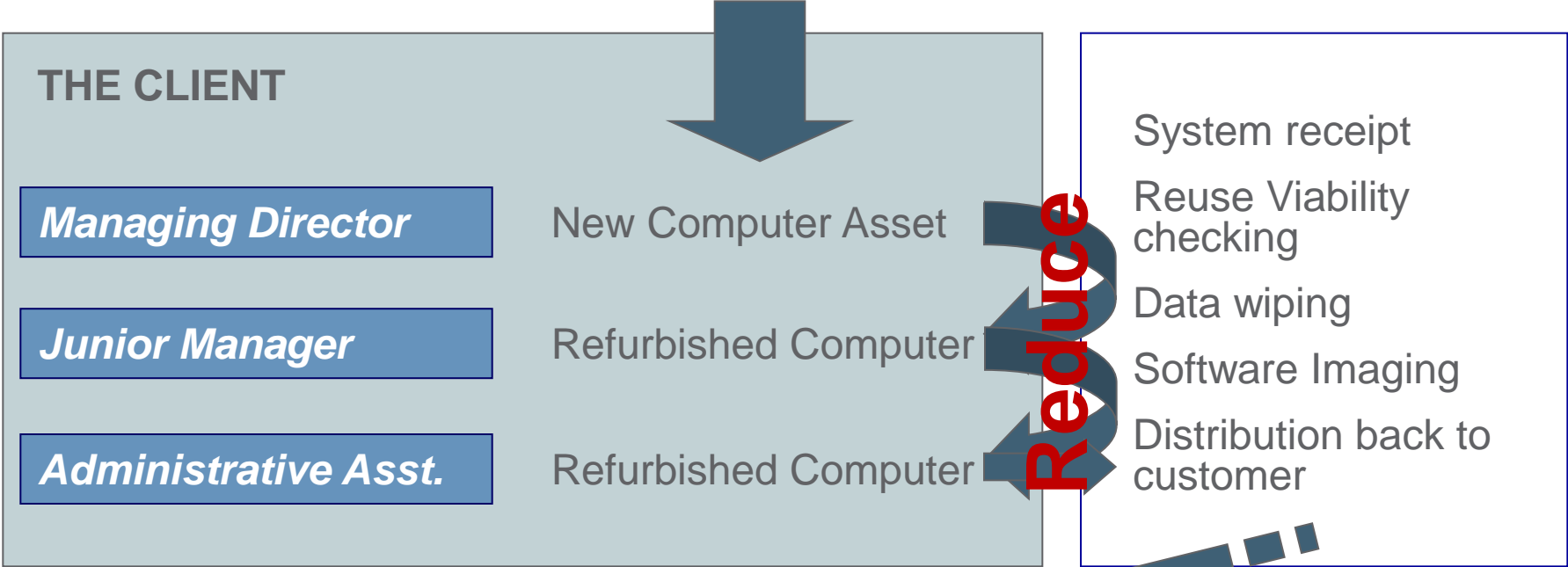


©2009 MichaelBluejay.com/electricity

# IT and legislation

- Legislation for creating greener IT
  - **RoHS Directive** – Restriction of Hazardous Substances (IT must be manufactured without certain identified hazardous materials)
  - **Energy using Products Directive** (a directive driving the Eco-friendly design of IT equipment)
  - **Batteries Directive** (ensuring batteries are being recycled and use of hazardous materials are controlled)
  - **WEEE Directive** – Individual Producer Responsibility (a future development encouraging producers to achieve cost savings with easier to recycle products)
- Legislation controlling the replacement of IT
  - **WEEE Directive** – producer responsibility for recycling IT
    - **Reduce, Reuse, Recycle**
- Duty of Care - aside from legislation
  - Legislation has created a new market for Electronic Recovery and Recycling (opportunists / professionals)

# Extending an asset's lifecycle within a business



**Reuse**



**Reuse**



**Recycle**



# Recovering an asset's resources at end of life

- **Reduce** – Redeploy current assets within organisation
- **Re-use** – Data-wiping, refurbishing and re-sale / donation; Microsoft Authorised Refurbisher (MAR status)
- **Re-use** – Hand dismantling to recover components
  - Hard drives; memory, CPUs, Motherboards, etc.
- **Recycling** – material recovery rates as high as 95%
  - Hand dismantling for hazardous waste removal
    - Batteries, CRTs, LCD screens (fluorescent tubes), etc.
  - Mechanical processing
    - Ferrous metals; non-ferrous metals
  - Density processing through water table
    - copper wire; printed circuit boards; plastics and non-metallics
  - Polymer refinement:
    - PVC (Polyvinylchloride); Polypropylene / Polyethylene; ABS (Acrylonitrile Butadiene Styrene); Polystyrene
  - Cathode Ray Tube processing
    - Leaded glass cullet; Unleaded glass cullet; hazardous waste

# How does recycling help?

- If we re-use a computer, 1.8 tonnes of resource is saved by not making a new one
- For every computer recycled between 3 and 5 tonnes of Carbon Emissions are saved by re-using materials rather than producing virgin materials

Material	Energy Saving Terrajoules / 100,000 tonnes	CO2 abatement / 100,000 tonnes (% savings)
Aluminium	4460	354 (92%)
Copper	1060	81 (65%)
Ferrous	230	97 (58%)
Lead	987	161 (99%)
Nickel	1878	190 (90%)
Tin	1800	215 (99%)
Zinc	600	180 (76%)



**SIMS**  
RECYCLING  
SOLUTIONS

# Protecting your Data

# Data Protection Failures - Impact

- Data Breach
  - Your business critical information entering the public domain, or worse!
- Data Protection Act
  - Damaging your reputation by failing to protect your employees/customers
- Brand Damage and lost credibility
- Sarbanes Oxley
  - Peripheral involvement, as must prove financial records are accurate
- Market Demand
  - In certain second hand markets, value of Electronic equipment now depends on the quality and quantity of data it contains
- Damage to the auditing of systems and processes



# What equipment is at risk?

Items Covered	Risk Exposure
Desktops, Laptops, Servers	Hard drives containing confidential company information. Deleting does not delete files, reformatting still leaves accessible data.
Printers, Scanners, Copiers, Faxes	Many of these devices now have either an internal hard drive (around 4Gb – 20Gb) or a digital “flash” card (1Gb). This non-volatile memory stores the information on print jobs and is retained until overwritten
Other data storage media: DVD's, tapes, USB Sticks	All contain company data that is retrievable
Communications devices – Mobile phones /PDAs /Blackberries /GPS	As above including personal data on bank accounts etc, contacts and emailed documents plus satellite navigation data on home (& other) addresses.
Network equipment – routers, switches	Not company data but do contain network-specific data such as static IP addresses which expose networks to external risk of infiltration.
Point of sale, retail debit/credit terminals	May contain personal credit/debit information
Specialist equipment – medical and military equipment, etc.	May contain data specific to use (patient data) or encryption keys, etc.

# Data Destruction - terminology

- CESG (Communications Electronic Security Group)
  - National Technical Authority for Information Assurance
  - Concerned with data security through software deletion & degaussing
- Impact Levels (IL) – the potential risk data poses
- Secure Sanitisation Levels (SSL) – level of data deletion required
- High/Low security – general reference to levels of security in data deletion

Impact Level (IL)	IL Descriptor of Data	Secure Sanitisation Level (SSL)	High or low security
6	Top Secret	SSL3	High
5	Secret	SSL3	High
4	Confidential	SSL2	High
3	Restricted	SSL2	Low
2	Protect	SSL1	Low
1	Protect	SSL1	Low

# Data Destruction – Software based

- Guidance on secure data destruction is detailed in:
  - **HMG IA Standard No. 5**
    - Secure Sanitisation of Protectively Marked or Sensitive Information – March 2009, Issue 3.0
    - Set standards for data erasure on magnetic, semiconductor and optical media through overwriting and degaussing
- Examples of bespoke software certified by CESG
  - Blancco, DESlock, IBAS Expert Eraser, Kroll Ontrack, UltraErase
- Capable of SSL1 – SSL3 depending on the software solution
- Systems tested and ratified by QinetiQ

# Data Destruction – Hardware based, Degaussers

- Equipment that generates a magnetic field powerful enough to destroy magnetically stored information on hard drives or solid state memory devices
- Coercivity – is the power of the magnetic field required to reduce the materials magnetisation to zero, some equipment requires higher ratings than other equipment (measured in Oersteds, Oe)
- The CESG standard approves equipment for both the higher and lower levels of security
- Degaussers must be tested and retested:
  - Initially; whenever required by CESG; regular user testing
- Examples of Degaussers approved by CESG:
  - Hard Disk Magnet Crusher; Verity; Weircliffe;

# Data Destruction – Physical destruction

- Generally refers to the use of a hammer mill, shredder or granulator to reduce equipment to flakes
- Government recognised standards require these flakes to be less than 6mm in size
- With right systems in place, these systems are capable of safely destroying up to IL6
- Often the “granulated” material is then sent to recovery facility
  - Mixed with other high grade material
  - Processed into constituent materials via magnet systems, etc.

# Data Security – the Process

- Security Check (SC)
  - Most widely recognised security clearance for personnel in frequent and uncontrolled contact with secret assets and even top secret information
  - Involves a basic security clearance check (thorough vetting of CV and identification documents), checks against UK criminal and security records (if appropriate overseas) and credit checks
- Does your provider supply you with the necessary information to control your risk?
  - Paper trail from point of collection to point of destruction and disposition
  - Asset tag removal, date data destroyed, make, model, serial numbers,
  - Loaded software and licenses application list to ratify licenses are out of use
  - Facts and figures on reuse, recycling, disposal, etc.
  - Open book pricing (transparent and auditable)
  - Direct access to the system to maintain control of your assets

# Onsite services data destruction services

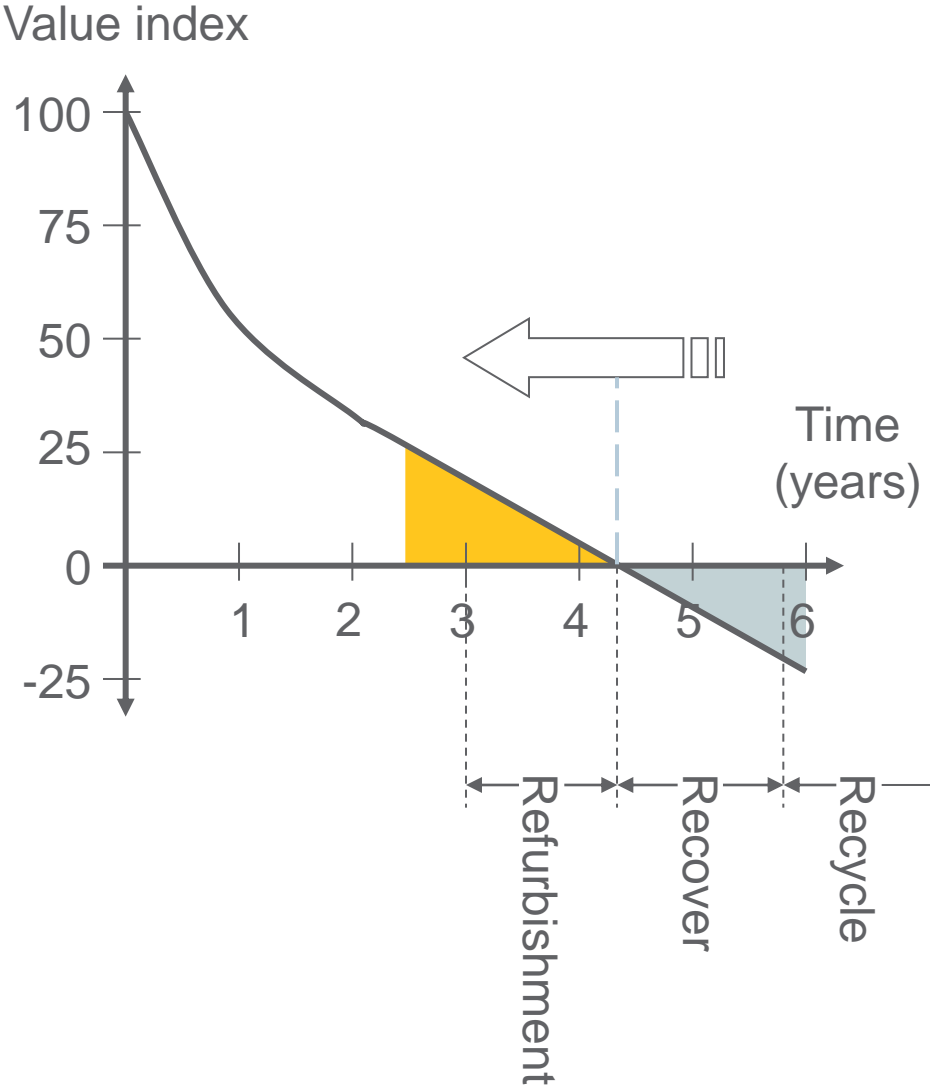
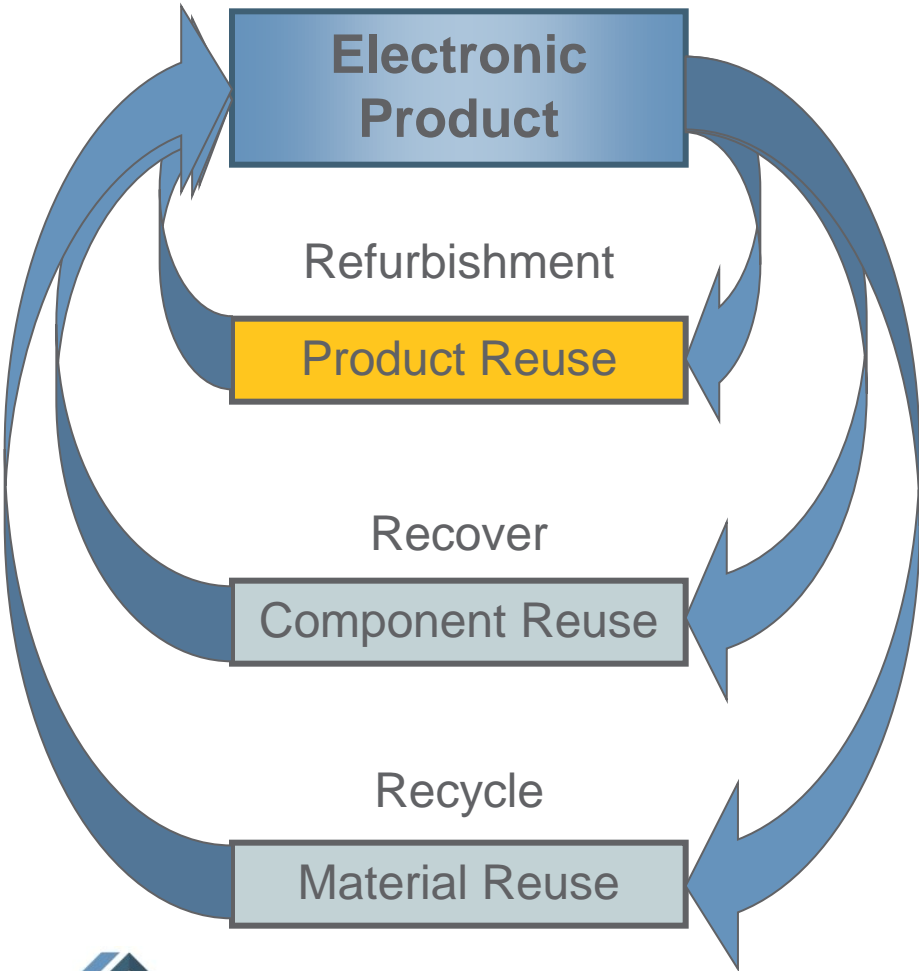
- On site is becoming the preferred option for clients with highly confidential data
  - Witness it destroyed before assets physically leave their site and control
- Industry is responding with a range of onsite services via transportable equipment operating to approved standards
  - Able to cope with all threat levels IL1 to IL6
  - Onsite service run by SC cleared personnel
  - Ultimate is the ability to physically destroy data bearing devices in line with Government standards for approved physical destruction
    - Less than 6mm sized granules
  - Able to offer software based data deletion – CESG standards
    - Certain products, such as Blancco, can be enacted through a network connection or by physically being taken on site



**SIMS**  
RECYCLING  
SOLUTIONS

# Protecting your Budget

# Extending the Lifecycle of assets



# Core Strategies

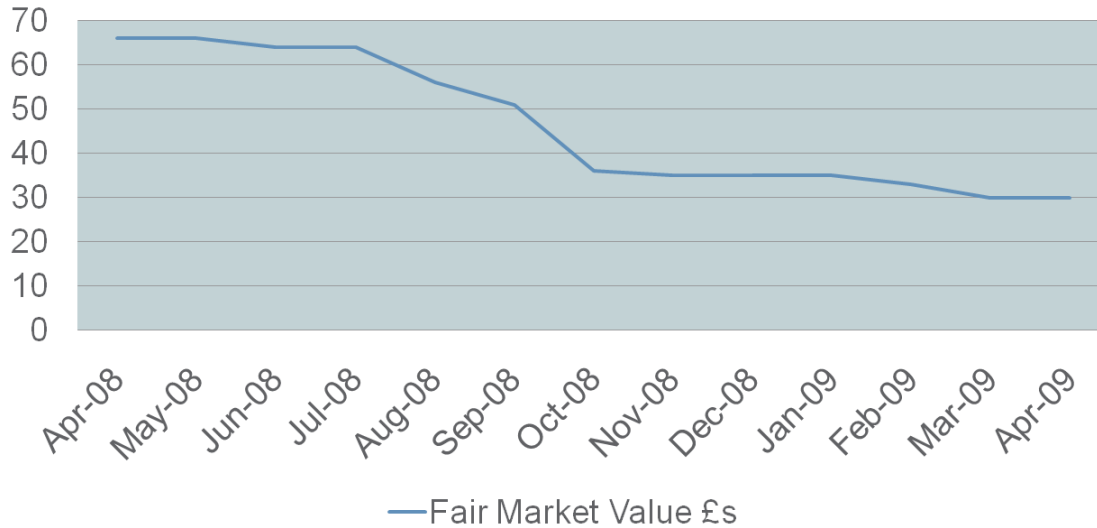
- Three core green IT business strategies
  - Best Environmental/Social Performance
  - Best Data Protection Performance
  - Best Price Performance
- Two main cost strategies
  - Guaranteed buy-back(positives and minuses)
    - Asset value is set at beginning of relationship based on an estimated worth at the end of their first phase life
    - Known value against which to depreciated the items
    - Potential “stealth” charges / not necessarily getting maximum asset value
  - Standard asset recovery model
    - Pay for service (SLA can then be controlled)
    - Transparent valuation of products ensure fair market value

# Costs involved

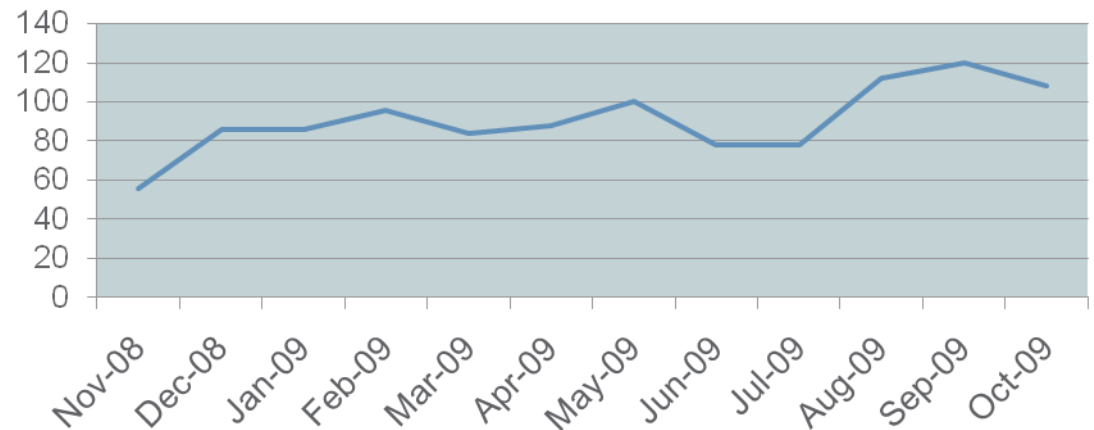
- **Logistics costs** – covers secure tracked vehicles, drivers that are by minimum CRB checked, if the request is for SC cleared drivers that is additional cost,
- **Processing costs** – all processing should take place at facilities which are physically secure
  - Full asset tracking of each individual unit received from arrival on site to final destination – reuse or recycle, using WebView
  - Data wiping – Blancco requires license cost on a per unit charge
  - Refurbishment of a unit in preparation for resale, picking and packing for resale
  - Recycling charges per unit (based on recovered material values, less charges for the treatment of any specific hazardous items)
- **Remarketing** - Service provider would retain a percentage of the Fair Market Value for assets... 70:30; or give an upfront estimate of potential future asset value

# Understanding Costs – Fair Market Value

## Pentium 4, 2.8GHz, 40Gb HD, 512 Mb RAM



## Ferrous Price Trends (OA)



# Case Study – Global Petrochemical Company

- Developed a comprehensive desktop refresh programme
- Core Strategy to achieve maximum return value
- Tied in with their new IT roll-out strategy, with estimated value returns to support their planning process
- After logistics and processing costs
  - UK - £272, 000 net of costs – 5221 units
    - (Average return of £52.09 per unit)
  - Europe – €29,000 net of costs – 1602 units
    - (Average return of €18.02 per unit)
  - USA - \$395,275.29 net of costs – 6155 units
    - (Average return of \$64.20 per unit)

# Summary

- ICT is getting greener, but this will create a short-term push reducing lifecycles of ICT
- Choose the core strategy for your electronic asset management
  - Data Security, Environment/CSR, Cost based
- Choose your preferred pricing option
  - Estimate up front / service charge with open book costs
- Choose your partner with care, based on your core strategy
  - Appropriate processing standards – Infosec 5, C ESG, ISO9001
- Do you have a fully audited electronic asset register?
- What are your asset reporting requirements – will they cross check with your asset register?

# Any Questions?

