

Transition Leaders Seminars – 11th July 2012

“The well-equipped professional”

Using technology sensibly to operate your own
business with minimum hassle

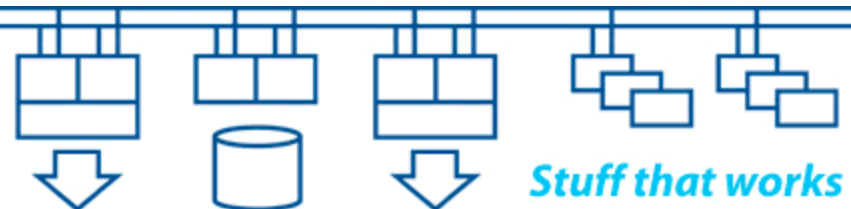
Colin Butcher

www.xdelta.co.uk



**transformation-
leaders**

Copyright © Colin Butcher, XDelta Limited, July 2012



Colin Butcher CEng FBCS CITP

Systems architect for mission critical systems (air traffic systems, healthcare, satellite ground control centres, power and utilities, finance data, etc.).

15+ years as independent consulting engineer.



Increase your level of understanding about computer systems and communications technology.

Improve how you work as a professional business.

Borrow ideas from other people's experiences.

This seminar is unlikely to answer all of your questions, so please be prepared to contribute and share your knowledge.

- Think about how you use technology and the effect it has on your professional appearance
- Understand more about the terminology
- Understand more about how things work
- Be safe – don't lose data
- Be secure – don't have unencrypted client data
- Improve your problem solving capability
- Q & A

- Keeping in touch with other people
- Document writing and exchange
- Finding and carrying information
- Software tools to help us do our work, for example:
 - Finance and accounting
 - Graphics design, photography and video
 - Data network trouble-shooting
 - Modelling and Data Analysis
 - Writing software
 - etc.
- Business administration (invoicing, banking, etc.)
- and so on ...

- What you have and how adept you are at using it is part of your professional appearance
- Your data and your systems are your responsibility. You have no-one else to blame. Invest accordingly.
- Your ability to function depends on your equipment being fully functional when you need it to be
- Need to interact easily and safely with your clients
- Safe data interchange and compatibility in whatever form the clients needs or provides
- Think about security and confidentiality. Ask first.

Types of Outage:	Planned (Maintenance)	Unplanned (Failure)
Hardware	?	?
Operating System	?	?
Application Software	?	?
Data	?	?
Connectivity	?	?
Upgrades & Updates	?	?
Users	?	?
Environment	?	?

- Things will fail. It will never be convenient. Be prepared. Have a “Plan B” (and C, and D, and ...).
- Hassle hurts an independent professional more than it does a bigger business. Plan ahead as best you can.
- Minimalism is good. Avoid complexity wherever possible.
- Know how to set your systems up. Know how to recreate them. Know how to back them up and restore them.

- Systems have a finite operational life. Plan accordingly.
- You generally get what you pay for. Budget accordingly.
- Even with a support contract – have enough alternatives to survive and be able to meet your client's expectations
- Stay reasonably current with hardware, firmware and software updates
- Make the effort to understand more and thus improve your ability to describe a problem

- How much capacity do you need ?
- What kind of performance do you need ?
- What connectivity do you need ?
- Most machines are slow because they have a slow storage subsystem (discs)
- Increase memory to minimise the need to go to disc (4GB maximum for 32bit)
- Solid-state disc has no moving parts = fast and reliable
- Disc controller with RAID and BBWBC = fast and reliable with a lot of storage

- The whole purpose of a backup is to be able to restore the data and the system quickly
- Practice your recovery procedures
- The two key components to consider:
 - System (difficult and time-consuming to recreate)
 - Data (sometimes impossible to recreate)
- Archives are useful for long term storage of data
- You need to keep the software that wrote the data in order to be able to read it one day
- Make two copies and keep one off-site

- Authentication – prove that you are who you are
- Encryption – protect access to sensitive information
- Strong passwords
- Digital certificates
- RSA fobs
- Web site transactions (HTTPS)
- E-mail
- Files (eg: PDFs)
- Whole disc encryption / container file encryption
- Portable storage encryption

- Mail flows between mail servers:
 - ISPs (Internet Service Provider)
 - Individual organisations
- Mail originates and terminates with mail clients
- SMTP (Simple Mail Transfer Protocol) to send (ideally authenticated)
- POP3 (Post Office Protocol Version 3) to receive
- IMAP (Internet Message Access Protocol) to look in mail folders on mail server
- Don't send big attachments – ever!

- Viruses are generally carried by e-mail or other files being exchanged between computers. Be highly suspicious of e-mails from anyone you don't recognise and never open attachments without scanning them.
- Anti-virus software **MUST** be kept up to date in order for the software to scan your files and e-mails successfully.
- The operating systems **MUST** be kept up to date by applying security updates and patches. Microsoft software tends to be particularly vulnerable.

- New desktop PC. What did I buy – and why?
- What software do I run – and why?
- New portable PC. What did I get – and why?
- It mirrors my desktop PC as closely as possible.
- What add-ons are useful when travelling – and why?
- How do I connect to the ‘net’ and clients when in my office?
- How do I connect to the ‘net’ when travelling?

- Think big, implement small.
- Buy on functionality and reliability, not price.
- Buy carefully from reputable suppliers. You need to minimise hassle if there are problems.
- Invest in things that make your life easier.
- Take frequent backups of both your data and your system. The objective is minimal restore time.
- Regularly prove that your backups work.
- Avoid single points of failure wherever possible.
- Carry copies of your data separately.
- Don't be 100% dependent on technology.

Thank you for your participation

Colin Butcher

www.xdelta.co.uk