WHAT YOU NEED TO KNOW ABOUT YOUR SUPPLIER'S DATA PROTECTION STRATEGY

by Carole Edrich, Senior Consultant, Cutter Consortium
http://www.cutter.com/consultants/edrichc.html

Partnering with small to medium-sized companies as part of a sourcing approach or supply chain management strategy has become very common. The benefits include the security of supplier diversity, considerable leverage, excellent personal service, and the provision of niche goods and services. But all this comes to nothing if the supplier suffers service interruption or degradation as a result of inadequate data protection. So it is incumbent on the client to ensure that suppliers have a sufficient backup and recovery process in place.

In this Advisor, we'll examine some of the logic behind small to medium-sized company best practice data protection strategies. Clients can utilize this logic to evaluate the risks of working with potential suppliers.

A 2004 UK government survey found that over 90% of Britain's small to medium-sized business computer users failed to run sufficient back-up procedures to ensure minimal business interruption, and over 35% suffered significant data loss as a result. These businesses believed they had adequate data recovery (DR) procedures in place before disaster struck and they were tested. A similar survey in the US found that 30% of small to medium-sized US businesses have no DR strategy at all, 64% admit that their backup and DR plans have significant vulnerabilities, 40% don't test their plans regularly, and 28% have never tested anything at all.

While most people understand the need to back up their files, they rarely consider the importance of keeping copies in suitable remote locations and, until it's too late, don't appreciate that the whole process should be done regularly and without fail. This becomes all the more critical when a partner's data is involved. Any system that requires intervention or that places its backed up data in the same location is prone to human error and at the same time leaves both copies liable to localized hazards.

An efficient and error-free restore process is vital, since failed restore from manual backups is an unfortunately common occurrence resulting in losses valued at millions of dollars each year. This means that manual or local automated systems are only marginally better than leaving it to up to individual staff to take copies as and when they remember, as each leaves data nearly as exposed as though the backups were not done at all. It therefore makes more sense to consider an automated remote backup service, but it's important that the service provides more than the ability to keep endless backup copies in a remote environment.

Since data sometimes corrupts or a virus may be taken on board days before it's noticed, it's important to be able to go back to a version that is known to be safe and secure. The ability to provide an adequate number of iterations to ensure that restored data is as close as possible to what was lost is a must. A minimum of 20 iterations should be considered, with 30 to 60 ideal. The more the better, since they provide a better level of flexibility and ensure that restored data will be as current and comprehensive as possible.

The software itself should be intuitive and easy to use. It should allow the user to set up both regular and ad-hoc backups as well as full and differential ones that include facilities for different document versions, file names, and content changes (incremental backups do not use space as effectively, so can be discounted from the selection process unless a user has very specific requirements). Backups should optionally cover every single identifiable byte on the source computer, including batch files, e-mails, and hidden files. It should also be able to select whether or not to receive notification of important stages and events in the process and e-mail is the only practical way to do this.

Archived data should be easily viewed, the restore process should preserve original files and their paths and it should be possible to retrieve files at any time. The charge should be as low as possible but sufficiently flexible to allow for growing data needs, thus ensuring that minimal overheads are passed on to the outsourcing or supply chain client. Stored information should be compressed to save on space and therefore cost. Since personal and critical business information will be stored, the highest level of encryption formats is sensible, with access permitted through personal keys or passwords.

Adopting an automated service that just backs up data to one other place, however secure, is also dangerous since even the most secure location might fall prey to unanticipated problems. Two offsite storage areas are a minimum and three are more secure, since in the event that one entire location is compromised, data is still protected and maintained in the other two. Each storage center should be monitored 24-7, be in different buildings, different geographical areas, and as secure as possible. It's therefore useful to look for a guarantee of the number of servers by the provider.

An English company called **DepositIt** has three, and its servers are served by IPs connected through a VPN thus providing yet another barrier to public access. Since each server runs RAID5, this allows for immediate hot swappable hard drives in the event of one failing. Security accreditation of the remote provider is also important, and the client auditor should look for good protection against trespass, fire, flood, and power interruptions.

Data should be transferred using SSL (Secure Socket Layers), which is considered sufficiently secure for Internet banking file transfers. It is not necessarily vital to find a service that is completely ISO 17799 compliant since maintaining compliance is likely to add to the overall cost of the service and be passed on to clients and customers. However, an extremely detailed and comprehensive internal standard, showing that every potential point of failure has been considered and defended, coupled with comprehensive service-level criteria for Internet and virtual network provision and security is vital. A demonstrable and regularly certified level of security from remote service providers should also be implemented across facilities, operations, and continuity and control services.

The software should take up minimal space on disc and RAM, should not be intrusive to the user, and should run on all common operating systems with firewalls running. There should be no opportunity to compromise data or activate unidentified viruses with backed up data, so other uses (such as file sharing, public ftp, or any file activation common with a number of US services) of the secure storage areas should

on no account be supported. Providing fast data transmission such as Broadband is employed, it makes no difference what country or area in which the provider is located, although there is extra security for stored data held as far from the business as practical. For larger enterprises it is important that the software can be used over a LAN or WAN and service co-located servers hosted in other remote data centers.

While a number of remote backup service providers such as Protect-data.com, Vispa.net, Ziptonet.com, Storegate.co.uk, Datafort, and DespositIt, backupmystuff.co.uk and backupdirect.net all offer similar services, **DepositIt** appears to fulfil all of the requirements at an incredibly low price.

In addition to full and incremental backups, the company uses delta blocking technology for differential backups, ensuring that only the relevant part of any changed file is transferred to the servers, thus freeing bandwidth for other operations as well as decreasing the time required for each backup (daily, hourly, etc.).

Additional encryption will provide the smaller business with another level of confidence. David Ryb of DepositIt says that they decided to encrypt and compress the data once at the client side and again to 448-bit level when stored on the secure servers for extra security. The fact that this is a stronger level than that used by most of the Internet banking industry could be considered overkill but is also an indication that the company is serious.

However, even though the logic behind remote backup is clear, different organizations will still have different requirement specifications to cater to their individual needs and priorities. What is therefore important is that the sourcing manager is happy with the supplier's logic in its strategy, the way it acquires, tests, and maintains its remote backup solutions. The prudent client will therefore examine the supplier's data protection strategy and technology as part of the supplier evaluation process and consider including clauses that provide periodic access to business continuity and disaster recovery audits as well as those covering protection of client and supplier data.

-- Carole Edrich, Senior Consultant, Cutter Consortium
http://www.cutter.com/consultants/edrichc.html

About Carole Edrich:
With over 17 years consulting in the management of risk, change and corporate governance, Carole Edrich decided that it was time to change in her life and became a full time writer. Author of three books on risk management, one on software development tools and numerous papers in the *mainstream press*, *Strategic Risk, IT Week*, *Risk*, *Risk Professional* and *Parliamentary Review* inter alia, Ms. Edrich has also appeared on television and radio, including CNN, BBC radio 4, Five Live, ABC, and ITV and; working through the UN, was instrumental in creating and coordinating the Maldivian tsunami emergency recovery centres.

Founder and Principal of KAI Corporation (Risk); a successful international risk management consultancy, she has worked in major national and international organisations in both private and public sector, was responsible for creating, developing and running the UK Central Government's risk management syllabus and accreditation process (M_o_R), has been instrumental in the creation of several university courses, is on the editorial board of several prestigious academic journals (such as the Journal of Corporate Governance and Control) and is still an internationally acknowledged thought-leader in big-picture risk management.

Every single project and programme with which she has been involved was completed on time, to budget and with the client's entire satisfaction. This was done by application of her own Systemic Risk Management methodology (the world's first, although she didn't realise it at the time) and through a thorough and pragmatic understanding of programme and project management and human behavioural psychology.

Carole also writes about global issues (through a sense of vocation), dance (because it's fun) and adventure and extreme sports (because she likes doing them), speaks Spanish, Dutch and French well and other languages to varying levels.

For enquiries or information, contact her at carole@caroleedrich.com or refer to the websites www.CaroleEdrich.com and www.webwandering.com.