

Family Office Technology: Top Ten things to know about IT and Using a Portfolio Approach to Technology for Wealth Management

by

Bryan Bell

President and Founder, Synth-Bank Consulting, LLC
IIRUSA, 16th Family Office Forum, Chicago, June 9, 2009



Overview

- 1) Take a Portfolio approach to selecting Applications and Services
- 2) Create a Strategic IT Plan
- 3) Decide what to Insource versus Outsource
- 4) Build a modern network- Firewall, broadband connections, cabling
- 5) Play Strong Defense- Anti-virus, Anti-spyware, Anti-spam
- 6) Replace hardware early and often
- 7) Create a Security program consisting of Products, Processes and People
- 8) Create Desktop Support program with Service Levels and a Help Log
- 9) Practice Offsite Backups
- 10) Have a Disaster Recovery Plan and keep it updated

1) Take a Portfolio approach to selecting Applications and Services

- Client Interview
 - Risk Tolerance, Time Horizon, Goals, Liquidity, Income needs
 - Investment Policy Statement
 - Strategic Asset allocation
 - Equities, Fixed Income, Private, Venture
- Implementation
- Ongoing Monitoring
- Performance risk

1) Take a Portfolio approach to selecting Applications and Services

- Business Interview
 - Risk tolerance, Time Horizon, Goals, Budget, Regulatory environment
- Technology Strategy
 - Application Allocation *See Threshold matrix
 - Desktop, communications, financial, knowledge mgmt.
- Implementation
 - Vendor Selection, Project Management, Staff Impact
- Ongoing maintenance
 - Monitoring Risk, performance, costs

1) Take a Portfolio approach to selecting Applications and Services

- Problems
 - Investment Problems-
 - Lose Money
 - Emotional attachment to a losing product
 - IT Problems –
 - Lose data, privacy, control, regulatory impact
 - Emotional attachment to a failing technology
- Opportunities
 - Just like the next great investment that was not planned you have to manage away from, pre-planned projects to find extra money for new technology
 - Discipline to stay the course and not be managed by press and fashion
 - Due Diligence methodology

2) Create a Strategic IT Plan

- Should look like an Investment Policy Statement
- Get professional help if you need this.
- Operating without a strategic plan is like investing in the next new thing without a portfolio strategy.

3) Decide what to Insource versus Outsource

- With IT costs soaring Outsourcing has become more attractive
- However Insourcing can still bring you the most control over your data and processes.
- Use risk management as a guideline when making these decisions
 - Think about what happens if the system is unavailable
 - Think about what happens if the system is compromised
 - Think about what happens when the relationship is over
- Read the Contract

4) Build a modern network

- Firewall appliance-should be a stand alone box and not part of any computer or server. Many systems come bundled with additional features such as the previous slide. Use of VPN tunnels will protect your data “over the wire” and between branch offices.
- Broadband connections-Now there are many alternative sources for getting broadband. Most carriers requires 1 or 2 year term but it is important to constantly reevaluate your needs and upgrade to meet the requirement.
- Cabling-should be at least CAT 5e or CAT 6 to handle today’s network speeds. Always test every jack and cable in the entire system at least one time to be sure all a cables are good. Test all cables that are purchased later. Troubleshoot can be a nightmare if you don’t first have proof the cable is not at fault.
- Wireless Connections- Wireless should be thought through carefully with planning in regards to security, stability and channel interference with other devices.

5) Play Strong Defense

- Anti-virus, Anti-virus systems are working on a daily basis to identify threats. It is crucial to have active subscriptions on all machines and the mail/fileservers.
- Anti-spyware, Drive by websites have become the #1 offender in placing spyware onto your machines. Understand this practice and purchase the latest tools.
- Anti-spam, is an imperfect science and there is no long term solution. There will always be spam and false positive and negative results. Find a user friendly tool. Decide if the users or administrators will handle the issue. Spam is a major source of phishing, viruses and spyware.

6) Replace hardware early and often

- 2 years is the optimal length for primary usage of a new computer
- Match machine performance to task requirements
- Computers can be down streamed to lower functioning applications
- Study total cost of ownership – not simply hardware purchase prices
- Maintaining old hardware can be very expensive such as a 4 hour service call per incident
- Always totally erase machines before decommissioning or donating

7) Create a Security program

- Products-firewalls, audit logging, access control of master systems
- Processes-need to know basis for accessing information, write protecting removable media, no application passwords for system level access people, standard financial controls and oversight, process for deactivating upon termination
- People- people are the biggest risk to major loss. Background checks in hiring, monitoring, financial controls, policies

8) Create Desktop Support program

- Service Levels-there hardest part of desktop support is managing the expectations of what services are “in or out” of the support program, desktops, cell phones, pdas, home machines, projects, help desk, training, associates and clients. At Threshold we have an very inclusive program. Other offices may a less inclusive approach.
- Help Log- Have a simple method of placing and tracking work orders for internal and external customers. This helps you with cost control, managing priorities and reporting on accomplishments.
- Plan upgrades and repairs. There will always be last minute activities in IT but the more you can manage the timing the less often you have to “throw money at a problem” .

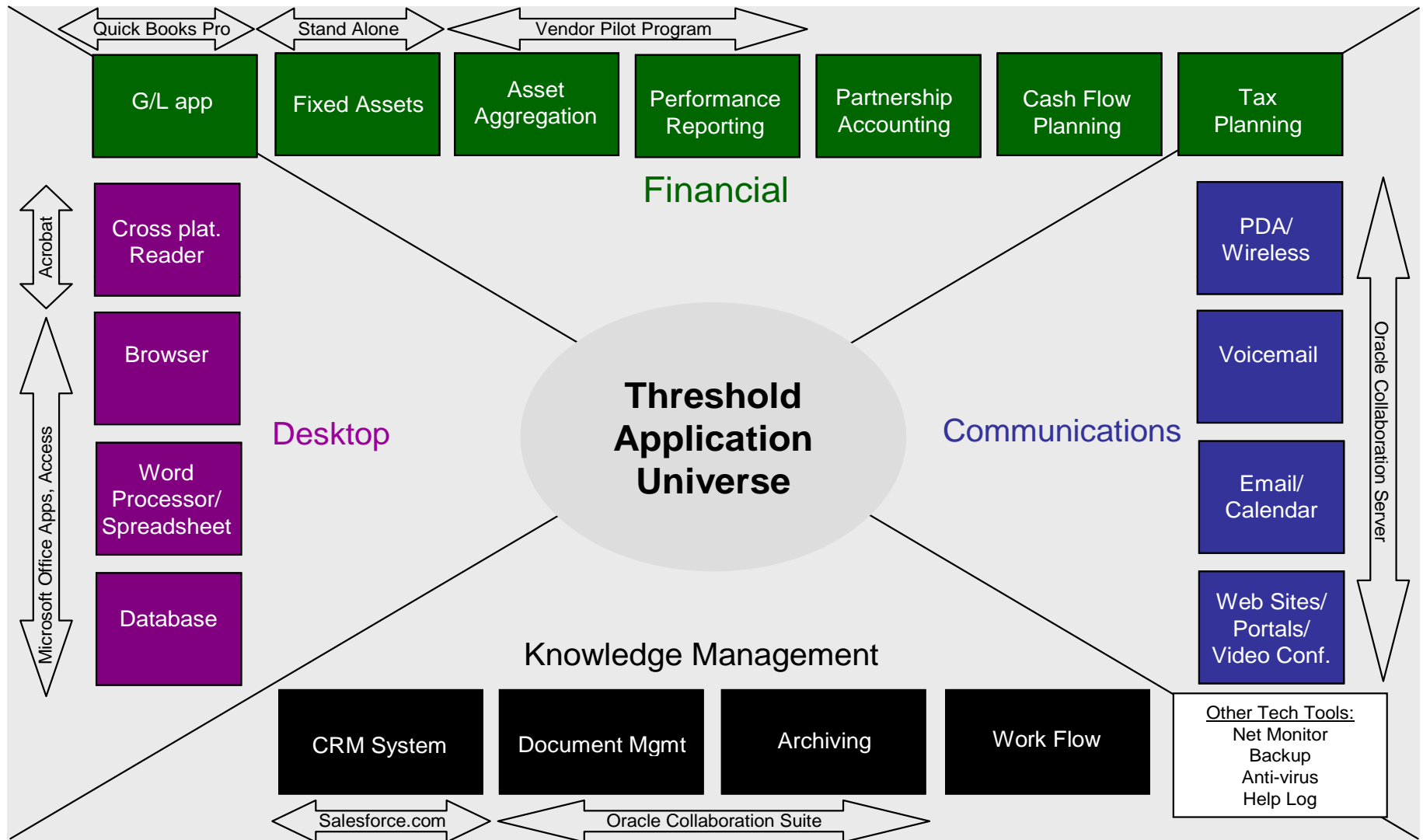
9) Practice Offsite Backups

- How backups differ from an archive
- A Backup is primarily designed to bring a system back to a specific point in time – for example last Thursday evening. If you delete a memo on Wednesday and bring back the Thursday backup the memo will still be gone.
- An Archive is designed to have long term persistent storage as to the state of a document or item at a given point in time. For example a memo sent to a client on July 1, 2007. Family offices are often covered by regulations around financial matters and have specific requirements for archiving books and records that are not met by most backup packages.
- Document management systems and CRM systems all have some archival capabilities but are rarely used properly to accomplish true archive capability.
- Store at least 1 copy of your data in a “hardened” offsite facility.

10) Have a Disaster Recovery Plan

- How is DR different from a backup? A backup is simply a “copy” of the data. Disaster Recovery implies that you have all of the pieces to recreate the entire environment, systems, processes, people and data to operate the business after an incident.
- Create a comprehensive plan of systems, data, people, processes to completely restore the operations to the desired levels. Scenario planning is often the best way to develop different DR requirements. A) building is OK – no entry permitted B) town is damaged such as bridges etc. C) regional disaster such as flooding, tsunami, earthquake
- Test it- best practices for DR drills should be performed annually.
- Keep it updated-because systems and people are always changing it is important to be sure that your DR plan reflects any changes that make it into production.

Technology Infrastructure – Framework for Service



Questions

- Bryan Bell
- bbell@synthbank.com
- 253 255 6625

