

Revenue On-Line Service

- **Introduction**

- Colm Bermingham, ROS Project Manager
- Jack Nagle, Baltimore Technologies

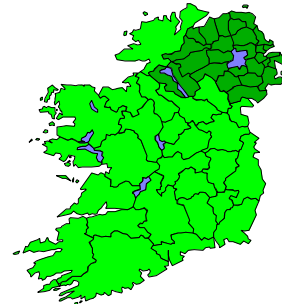
- **Today's Presentation**

- Background to ROS
- Business considerations for Disaster Recovery and Business Continuity
- Irish Revenue's Disaster Recovery solution
- Technical considerations for Disaster Recovery
- Other DR scenarios



ROS – Background IRELAND

- Land area <0.75% size of U.S.
- Population 4 million
- Revenue Commissioners = IRS
- Taxes
 - Sales, Payroll, Income, Corporation
 - Capital Gains, Excise, Capital Taxes
- Yield in 2001 – \$37,596m.



ROS – Background

- **DRIVERS**

- Revenue Board Statement of Strategy 1997 - 1999
 - 50% of all business returns filed electronically by 2005
 - Position ROS as the preferred method by which customers interact with Revenue
- eGovernment Initiative
 - Information Society Commission
 - National eBroker projects for Corporations & Citizens
 - European Union Benchmarking



ROS – Background

- **ROS So Far**

- Board approval Jan 1999
- Contractors
 - Accenture (Developers) appointed Jan 2000
 - Baltimore (Security) appointed May 2000
- Aggressive schedule – **LIVE** on September 29th 2000
- Annual target reached in 8 weeks.
- 55% of Customer base – 15% of tax yield
- \$4,000,000,000 (\$4Bn) payments received
- Over \$300,000,000 refunded



ROS – Services

- **Filing Tax Returns**
 - Payroll Tax, Sales Tax
 - Income Tax & Corporation Tax
- **Making Payments**
- **Access to Tax Information**
 - Own Revenue data
- **Access Control System**
 - Agents and Corporations

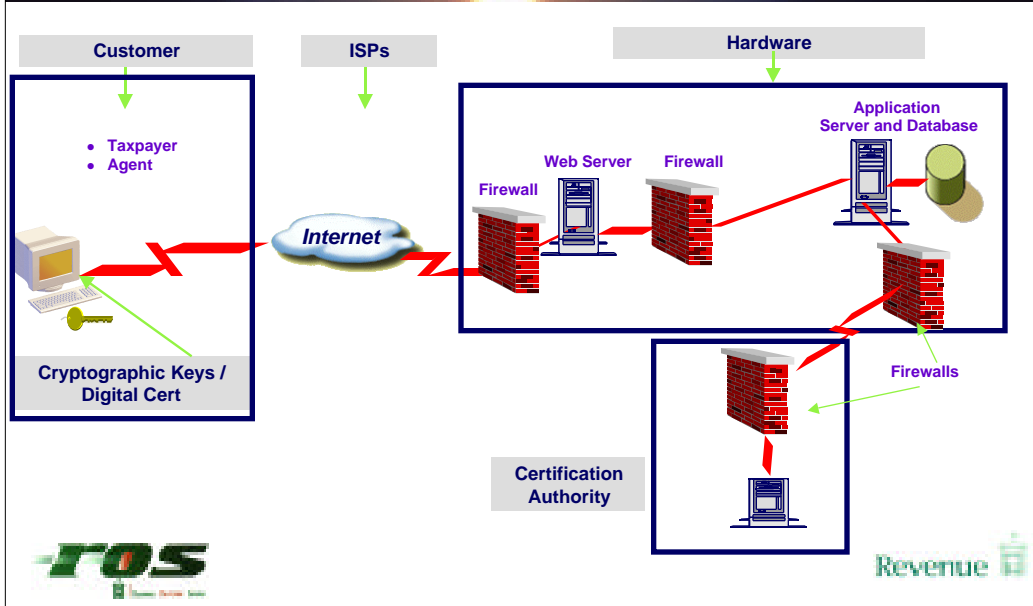


ROS – DR Planning

- **Business considerations**
 - What is a “Disaster”?
 - Customer perspective
 - Revenue perspective
 - What can be predicted?
 - What elements can we control?
 - Cost
 - Systems
 - Testing
 - Business Continuity plan
 - PR plan for various scenarios



ROS – Components



ROS – DR – Summary

• Disaster Preparedness and Recovery

- Quantify “Disaster”
- Identify critical components/issues
- Ensure effective DR plans for all in your chain
- PR plan

Disaster Recovery A Vendor's Perspective

- Disaster Recovery and Business Continuity Planning
- Disaster Recovery Planning
- ROS Disaster Recovery
- General Comments on the ROS DR solution
- Nature of Disasters (systemic and otherwise)
- Key Messages



Disaster Recovery Business Continuity Planning

- Goes beyond security issues in terms of policy breach or unauthorised access
- About contingency planning for business threatening emergency
- About continuing business in the event of a disaster
- BCP – about making plans to allow business continue
- DRP – about recovering from an emergency with minimum of impact



Disaster Recovery Planning

“A disaster recovery plan is a comprehensive statement of consistent actions to be taken before, during and after a disruptive event that causes a significant loss of information systems resources. Disaster Recovery Plans are the procedures for responding to an emergency, providing extended backup operations during the interruption, and managing recovery and salvage processes afterwards, should an organisation experience a substantial loss of processing capability.”

CISSP Prep Guide 2001



Disaster Recovery Planning

- Main goals;
 - Reduce confusion
 - Provide an organised way in which to make decisions
- Done properly can;
 - Protect an organisation from major computer services failure
 - Minimise risk as a result of delays
 - Guarantee the reliability of standby systems through testing and simulation
 - Minimise decision-making required by personnel during a disaster (good judgement still a must)



ROS Disaster Recovery

- Core PKI system is housed in an accredited secure hosting environment
- Classes of failure
 - Database machine (Treated as a separate item because of its criticality)
 - Machine Failure
 - Loss of facility (Destruction of Hosting Site)



ROS Disaster Recovery

What are we supposed to do now !!!

Help is at hand – we have a plan

- Database machine
 - Copy of Database on Backup1 machine
 - ROS Trusted elements
 - ROS Configuration Baseline (Private) document
 - Hardening and Recovery (Private) document
 - ROS PKI Configuration (Private) document



ROS Disaster Recovery

- Loss of Facility
- Backup Facility
- Full set of backup material
 - Machines on site
 - Some core elements already in place i.e. LDAP
 - All other material available from secure off-site archive



General Comments on the ROS DR Solution

- The approach taken was based on;
 - Fitness of business purpose
 - Available resources
 - Relevant level of criticality i.e. not mission or life
 - Contingency planning for late filings
- Backup procedures have been shown to work to an acceptable level
- Organisational issues – consortium based project
 - Multiparty solution and single points of contact



Nature of Disasters (systemic and otherwise)

- By their nature unpredictable
- Possible to anticipate certain types of event may happen
- Disaster Prevention
 - Can be a big mistake to assume all is well
 - Example of 'systemic' failure in terms of backup configuration
 - Value of audit from the outset (my view)
 - Value of checking with auditors (offsite backup example)
- Overall importance of good design in terms of product choice and configuration
 - Poor anticipation of usage will overcome even a good product for example



Importance of Accreditation

- Why bother with standards and accreditation ?
 - Fundamental to 'preparedness' and prevention
 - Gives an objective reference point for best practice
 - Customer reassurance
- What's accredited?
 - People
 - Processes
 - Product



Accreditation

- Many Standards bodies
 - ANSI, NIST, ISO, IETF etc.
- Specifics for security products
 - Necessary from a continuity perspective
- Include FIPS (Hardware), BS/IS7799, SAS70 (People and Processes), ITSEC E3 (Software systems) etc.
- Conformance with legislation
 - Electronic Commerce Act 2000 which includes the status of systems and personnel
- Use hardened systems



Key Messages

- DRP and BCP go hand-in-hand
- Numerous ways of 'mixing and matching'
- Suitability of DR scheme for system requirements and available resources
- This is a joint presentation from a client and vendor
 - We have implemented a business critical system
 - We have implemented a DRP
 - It has worked in test mode
 - More importantly it has worked in real-world mode
- From a user's perspective it provides an additional level of reassurance
- Good communication to users helps validate system integrity



ROS – Contacts

- **Colm Bermingham, ROS Project Manager**
 - ◆ cberming@revenue.ie
- **Jack Nagle, Baltimore – Public Sector Manager**
 - ◆ jnagle@baltimore.com
- **Margaret Whelan, ROS Strategy Manager**
 - ◆ marwhela@revenue.ie
- **Revenue** - **ROS**
www.revenue.ie - www.ros.ie

