



CERT-MU

The Importance of

Critical Information Infrastructure at national level

Monday 31 August 2009

Pete Frielinghaus
GM ContinuityMauritius

Our Business is Keeping you in Business



Why do we need to Protect Information?

- The Obvious Reasons
- What Information or Infrastructure are we talking about
 - National (WWW, Demographic Databases, Physical Access Cables etc)
 - Private (Company information, Public information etc)
- How to Protect this Information
 - Physically
 - Interruption of services
 - Theft or Damage
 - Cyber Attacks
 - Being Proactive?
 - Planning
 - Testing
- Who needs to protect information and at what levels
- Technology Companies only?

Our Business is Keeping you in Business



Case Study

London Stock Exchange

TradElect System Crash

(8th Sep 2008)

Our Business is Keeping you in Business



Some Background

What is a Stock (Securities) Exchange?

- An organisation which hosts a market where stocks, bonds, options and futures, and commodities are traded
- Originally a central location that traders would meet
- Proliferation of Electronic Communication Networks (ECNs) – for information and for the actual buying and selling
- Physical exchanges began to vanish
- Technically a financial institution
- Essentially exchanges offer a shared computer system for transacting
- Are on the cutting edge of performance, scalability and reliability
- Are extremely high profile and visible, when something happens at an Exchange everyone knows about it
- Great companies to learn lessons from



The London Stock Exchange (LSE)

- Has a history of more than 300 years
- Starting in Coffee Houses of 17th Century London
- Upgraded, expanded and moved several times
- Housed at Paternoster Square, since 2004
- 3rd Biggest Stock Exchange in the world, over 3,000 listed companies with a Market Cap of £ 3.5 trillion
- Essentially electronic (Approx. 440 full time staff)



Our Business is Keeping you in Business



The TradElec System

- Took more than 4 years and £40 million to develop
- Three main goals:
 - Speed: Transaction time reduced from 140ms to sub 10ms
 - Capacity: Increased 5-fold. Could handle trading volume of all European equities
 - Reliability: Microsoft claimed “100% reliability”, LSE offered five-9s SLA (99.999% uptime)
- Designed and implemented by Accenture on HP and Microsoft technology
- Active/Active processing at geographically diverse sites
- No single point of failure
- Launched June 2007
- Marketed to other Exchanges
- Implemented by the JSE



So What Happened?

- Sunday, 7th Sep 2008:
US Government Announces £110 billion bailout of Fannie Mae and Freddie Mac
- Monday, 8th Sep 2008:
 - Japan Nikkei 225 up 3%
 - Hong Kong Hang Seng up 4.3%
- 8am London time
 - LSE Markets open
 - Double normal trade
- 8:45 – Brokers complain of communications problems
- 9:15 – TradElect brought offline
 - Trading grinds to a halt
 - JSE offline before trading even starts
- 11:15 – System brought up in “Auction” mode
 - Trades can be entered but not executed (Essentially trading in the dark)
- 16:00 – TradElect functional again
- 16:30 – Markets close



The Impact

- The Exchange was down on a day that had promised to be one of the busiest and most lucrative days of the year
- Down for seven hours (99.999% = up for next 84 years)
- In 1hour 15minutes of trading stocks rose 3.5%, the actual impact is impossible to measure
- £3bn in lost trading
- £700,000 per brokerage firm in commission (“Hundreds of millions of pounds”)
- LSE reputational damage, as well as to Accenture and Microsoft



Lessons Learnt

- Not much, because the LSE still hasn't come clean on the cause:
"It was software-related, a coincidence, due to two processes we couldn't have foreseen. We've introduced a fix and we're confident it will not happen again."
The cause doesn't matter, this is a mindset problem
- Eventually all systems, no matter how resilient or redundant, will fail. It's only a matter of how often (once a day or once a century)
- "No single point of failure" is not the same as "cannot fail"
- Interdependent, high-performance systems are complex, difficult to manage and hard to repair while in use
One error will often cause a domino effect

A Paradigm Shift? HA vs. DR

- High-Availability (System Availability)
 - The reduction or elimination of single points of failure
 - Probably automatic and involving little human decision making
 - Reduces the likelihood of a catastrophic event
- Disaster Recovery (System Recovery)
 - Consistent recovery of an entire network to a specific point in time
 - Probably manual and requires extensively human decision making
 - Reduces the impact of a catastrophic event
- HA is not the extreme of DR, they are different approaches to different problems
- HA does not mitigate software bugs, data corruption and human error, and in some instances may compound the problem



Information Protection - The New Disaster Recovery

- Separate Dedicated Team
 - You shouldn't have to choose between working on resolving the production problem and recovering at the DR site
 - (Bartlett's Law) – "When things go wrong, people get stupider"
 - Highly experienced and well rehearsed
- DR should be a known
 - How long will it take to recover?
 - How much information / transactions will I lose?
 - Will there be degraded performance and for how long?
 - Will we be able to elegantly roll back to production?



The Way Forward

“Security is the business of everybody, and only with the cooperation of everyone, an intelligent policy, high-quality network infrastructure and consistent practices, will it be achievable.”



Thank You

Our Business is Keeping you in Business