

# Business Resilience Breakfast Address

# VOLT

Professional  
Services



10<sup>th</sup> November 2010

# Introduction

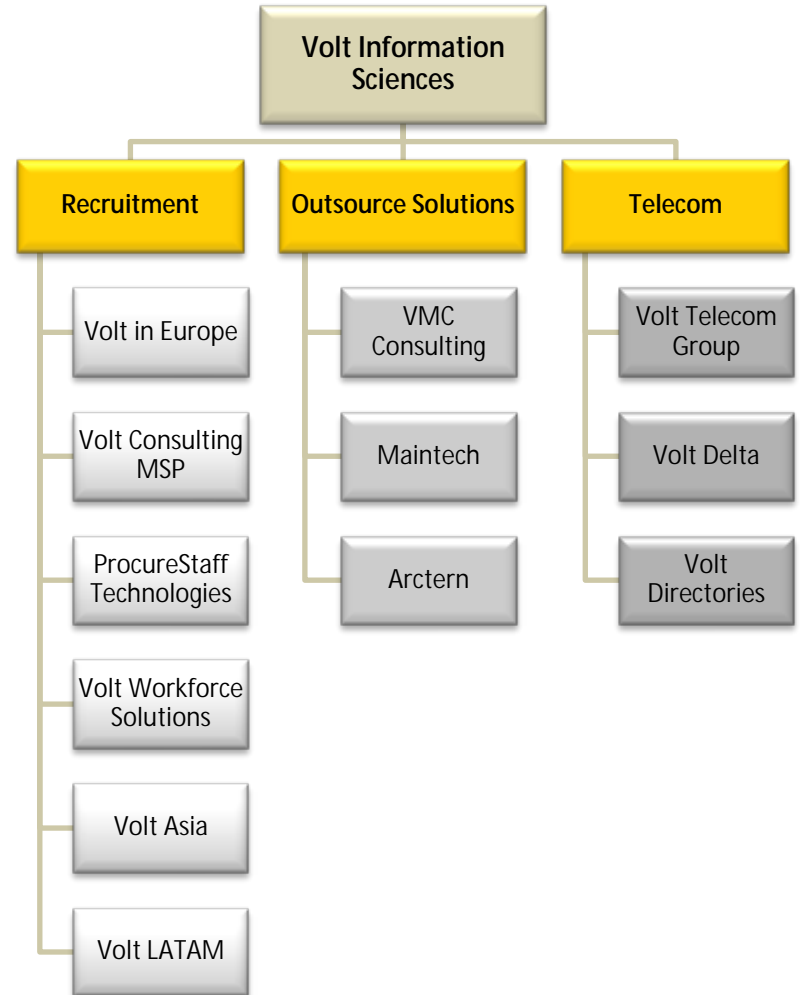
- Welcome: Dave Elliott-Smith
  - Purpose
  - Format
  - Housekeeping
  - Introductions to Speakers
  - Agenda

- Nigel Hall  
*“Strategic National and Business Resilience”*
- Q&A
- Dave Williams  
*“Cyber-specific Threat”*
- Q&A
- Nigel, David and Chris Baker  
*“Managing Complexity”*
- Closing remarks



# Volt – Celebrating 60 years of success

- P Volt Information Sciences
- P \$2.4 billion revenues
- P Trading since 1950
- P Listed on NYSE (VOL)
- P Global Staffing / Consultancy
- P Over 40,000 people on assignment daily
- P 300+ locations
- P Six Sigma Company



**VOLT**

# Volt Professional Services

- P Consolidation of Global Technical & Consulting offering in Europe
- P DNA Foundations
  - 4 **Open**, with Commercial **transparency**
  - 4 **Sophisticated** delivery model
  - 4 **Better, Faster** and More **Value**
- P Delivering change securely and supporting cost effective survival
  - 4 Programme and Project Management and Delivery
  - 4 Business Resilience
  - 4 Aim to make **expert** insight **accessible, affordable**, enhance Independent Assurance activities and promote **real time** top – down monitoring of **live risk status**



# VOLT

# High Profile Threats

## Defending Against Cyber Attacks

The Prime Minister, Rt. Hon. David Cameron, MP., states:

“We need to plan for pandemics, energy crises and water stoppages. And in particular for what I believe is a growing cyber threat.

We know that there are hundreds of thousands of cyber-attacks and crimes against British businesses every year. Against government and the public sector, there may be many more. As technology and computers and the internet become bigger and bigger parts of our lives, the effect of cyber warfare will become more pronounced.....

I want Britain to be prepared and proactive and ready to deal with all kinds of cyber attacks. So today we're announcing plans for a new Cyber Threat and Assessment Centre to provide exactly that”.

Source: <http://www.cybersecuritysummit.co.uk/> (accessed on 5<sup>th</sup> October, 2010).

# The Age of Digital Entanglement

“ON NOVEMBER 19, 2009, a single circuit board inside a computer router in Salt Lake City failed. The glitch cascaded, preventing air traffic control computers nationwide from communicating. Hundreds of flights were cancelled.

On May 6, 2010, the Dow Jones industrial average inexplicably plummeted almost 1,000 points in minutes, only to mysteriously rise before the day ended. Had the "flash crash" not reversed itself, a global financial meltdown would have ensued.

We humans have linked our destinies with our machines. Our technology has gotten so complex that we no longer can understand it or fully control it.”

*Daniel “Danny” Hillis, “What’s Next – Complexity”, Scientific American*



# A very dangerous cocktail

- > Internal terrorist threats
- > Revival in legacy Irish threat
- > Environmental crises
- > Threat to UK CNI
- > Enduring risk of pandemic
- > Single issue activists
- > Digital terror & E-Crime
- > Industrial espionage
- > Business travel
- > Extended supply chains
- > Disaffected employees



**VOLT**

# Fuse lit from within

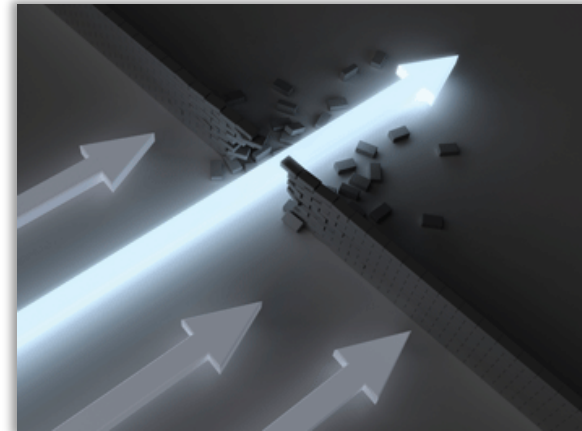
- M Social unrest, division...
- M Skills gap in expertise
- M London 2012
- M Complacency, complexity and Interdependency
- M Preoccupation with short-term imperatives
- M Too hard | Too £Much
- M Silo approach to risk
- M Reactive responses



**VOLT**

# Business Resilience Response

- 4 Independent & multi-disciplinary
- 4 Strategic insight
- 4 Stress Testing & Assurance
- 4 Support informed investments
- 4 Crisis Management
- 4 Incident Response teams
- 4 PM & Consulting
- 4 CLAS Consultants
- 4 Collaboration with CPNI funded  
Technology partners



For Volt this is a  
global priority.

**VOLT**



# From National Security to Homeland Resilience

Nigel Hall



# Need for Security & Resilience

## Why?

- L Urgency (natural & man-made)
- L Globalisation / interconnectivity / complexity
- L Failed & Failing states
- L Poverty & Humanitarian needs
- L Radicalisation & organised crime
- ê Global security
- ê Global Institutions
- ê Others' reliance/confidence in US
- ê Governance

# Agenda

- UK National Security
- National Security Action Priorities
- Homeland Resilience
- Homeland Resilience Action Priorities



# UK National Security

- Risk & Situation Awareness
- Science & Research
- Savvier balancing soft & hard power
- Much more agility and adaptability



# National Security Action Priorities

- Agile Government
- Ownership
- External Commission
- National Research Centre
- Research, Innovation & Education
- Arms Control & Disarmament



# Homeland Resilience

- Terrorism                   â
- Organised Crime           ã
- Cyber & E-Crime         ã
- Pandemics                   ã
- Flooding                     ã



# Homeland Resilience Action Priorities

- Risk & Situation Awareness
- National Command & Control
- Stress Testing
- Strategic Communications
- Cyber & E-Crime Effort
- Police Reform
- High Impact Event



# Final Thoughts



More Strategic and Agile  
More and Better Prepared  
Civil Society and Private Sector Roles

**VOLT**

Thank You



**VOLT**



# Keeping critical assets secure in today's cyber world

David Williams CLAS CISM CISSP



# Cyber threats

- More complexity
  - No real borders to speak of
  - Ability to utilise many 1000's of devices distributed throughout the world
- Can be from many sources
- Motivation varies
- It is real, can be bought as a service

# Challenge

- Ad-hoc integration across business units within the organisation
- Organisations lack situational awareness
- Organisations are complacent
- Perception – It will not happen to me
- Reactive approach to manage incidents

# Contributing factors

- Inconsistent levels of maturity within business units that are responsible for the delivery elements of the business process
- Risk assessments primarily look at impacts to Confidentiality, not Integrity or Availability
- Focus on gaining certifications than mitigating risks
- Checklist approach to certification

# Suggested objectives

- Ensure security and resilience are key deliverables within your business
- Executive level support
- Develop strategy to advance into a Self-Defending Business

# Attributes of a Self-Defending Business

- Fully understand the Threats they face
- Identified the key Risks to the business
- A highly integrated approach to treating Risk
- Proactively identify and respond to incidents
- Invest in key skills
- Increase situational awareness within staff
- Highly mature

# Summary

- The Threat to Your Business is real and it is a global problem
- Poor Integration, A Check List mentality and Low Security maturity is leaving business exposed and vulnerable
- Self-Defending businesses will be more resilient and effective in countering the Threats of the Digital age

Thank You



**VOLT**

# Closing Remarks

# VOLT

Professional  
Services

