UNITED KINGDOM (UK)
Cyber Security Market
• Government classified cyber security as ‘Tier 1’ national security risk
• National Cyber Security Program, initial outlay of $1 billion
• Highly networked nation, $75 billion online transactions/yr
• 87% of small firms, 93% large firms risked in 2012
• Demand from government and private sector
ALLOCATION OF CYBERSECURITY EXPENDITURES

SOURCE: ZDNET, 2013. DEVELOPED FROM ESTIMATES PROVIDED BY VARIOUS UK GOVERNMENT REPORTS AND PUBLISHED ARTICLES

Cyber security spending plans

- 65% Cyber capabilities
- 20% Critical cyber infrastructure
- 5% Cybercrime
- 1% Reserves
- 9% Education
MARKET ACCESS

- Close political, defense ally of USA
- Open access for US exporters to UK defense contracts
- UK-US Defense Trade Cooperation, licenses for defense equipment and services eliminated for sales to government
- Common language, cultural similarities
# UK CYBER SECURITY MARKET AT A GLANCE

## Strengths
- Strong political and defense relationship with the US
- Open and transparent market access
- Member of WTO’s Government Procurement Agreement

## Weaknesses
- Political issues with the EU
- Coalition government
- Expensive market to do business
- Compliance with UK laws and EU Directives

## Opportunities
- Increased spending on cyber security
- Access to the European Union market
- Private sector opportunities

## Threats
- Significant competition from other domestic and foreign companies
- Defense spending cuts
MARKET OPPORTUNITIES

• Niche market
• Opportunities → cloud computing, business analytics, anti-virus, content management, cyber security software and services
• Demand for ‘innovative’ cyber security solutions from experienced suppliers
DOING BUSINESS WITH GOVERNMENT

- Defence Equipment and Support (DE&S) agency of Ministry of Defence tasked with procurement of equipment and services for defense
- Significant competition for government contracts
- Exporters should abide by EU directives also