AN INTRODUCTION
Research and Innovation

<table>
<thead>
<tr>
<th>Director</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial Director and Business Development Team</td>
</tr>
<tr>
<td>Globally Leading Research Academics, RAs, PhDs</td>
</tr>
<tr>
<td>Senior Industry Experienced Engineering Staff</td>
</tr>
<tr>
<td>New Technology Products and Business Opportunities</td>
</tr>
</tbody>
</table>

- Internationally leading research – in carefully selected areas
- Work with industry – share longer term road-maps – “over the horizon view”
- Ambitious “mission and team” based research that address major problems
- Seeking potentially disruptive market opportunities
- Critical mass of experience engineering staff working alongside academic researchers
- Promote inflows and outflows of knowledge to accelerate innovation
Open Innovation Model
10 COMMERCIALLY RELEVANT NEW TECHNOLOGIES DEVELOPED

3 SPIN-OUTS:
- Titan IC Systems
- Activ Wireless
- MicroSense

STRONG SME CAPACITY

SUPPORT
RepKnight, AirPos, Seven, Cyberlytic, Titan IC, Netronome etc. have won significant new business because of CSIT

FOREIGN DIRECT INVESTMENT
- SUPPORTED UKTI AND INVEST NI SECURE 879 NEW JOBS IN THE SECTOR, (365 IN THE PIPELINE)
ECIT/CSIT + Science Park – 10+ years on
Cybersecurity research: a vision for the UK

Finance Challenges

Professor John McCanny
CBE FRS FREng
Research on Cyber Security Risk Management

Challenges

• Corporate Governance - little correlation between spending levels and maturity of cyber security risk management. Many organisations simply throwing money at problem

• Organisations treat as an operational risk but need to treat as an enterprise risk acknowledging the strategic value of their data – becomes a corporate governance board room issue

• Research community lacks a foundational understanding of a cyber secure organisation (including technology, people and processes)

Recommendations

• Research to help organisations understand cyber risks as an enterprise risk and to integrate into corporate governance to support/enhance business

• Identify quantitative metrics that set out type of data to be collected and methodologies for doing so for organisation types and industry sector – building on extensive research for assessing financial risk

• Convene research community and security professionals and risk manager to review “established knowledge”. Identify new products and services and ensure evidence base informs research exploitation.

• Research on the economics of networked organisations to inform aggregated risk management and new business models needed
Recommendations continued

• Managing systemic risks – financial sector has developed models to understand systemic risk, much less developed for Cyber Security. System wide governance and crisis management structures exist for international finance. Need to extend to Cyber Space.

• Cybersecurity stress testing provides an opportunity to help establish an evidence base to inform the cybersecurity risk management and investments.
  • To ensure the Bank of England’s framework is robust, the metrics involved should involve not only technical but also non-technical (management, organisational, psychological and sociological indicators) informed by interdisciplinary research.

• Opportunity for research community and insurance industry to tackle the challenge of aggregated and systemic risk management and consider the feasibility of international governance mechanisms.

• Opportunity for a research on building organisational resilience in cyberspace e.g. could involve government and industry funds but also business enterprises, such as insurers and major consultancies.

• Similar to Banks- to big to fail – Cyber Security aggregated risk management of Critical National Infrastructure (CNI)