



DR JOHN LEACH

PERSONAL DETAILS

Date of Birth: 21st July 1956

Education: BA Natural Sciences, Christ's College Cambridge, 1977
Diploma in Mathematics, Christ's College Cambridge, 1978
MA Natural Sciences, Christ's College Cambridge, 1979
Ph.D. Astrophysics, Stanford University, CA, 1983

Years in Info. Sec. 25+

Domestic: Married with children, living in Hampshire, Southern England

CAPABILITY AND EXPERIENCE

SUMMARY

I am an acknowledged Information Risk and Security expert with over 25 years' experience helping Blue Chip clients address strategic risk management problems and build enterprise-wide security improvement programmes.

I have a deep technical background (including a science Ph.D.) plus a wealth of experience in the security risk management field. This enables me to work closely with technical people whilst assisting top-level security and business management to address pressing security needs. I can communicate the value and benefits of improved security to C-level business management, design security programmes in response to governance and business objectives, and deliver improved security management systems and technical controls. I have helped clients in the areas of Security Governance, Security and Controls Frameworks, Identity Assurance, Privacy Protection, Risk Modelling, Risk Metrics and Dashboards, Security Monitoring, and the use of security data to create meaningful results and improve risk management decision making.

I continues to provide consultancy services across a wide range of topics in the risk management and security field. My mission is to provide innovative thought leadership and high-value consulting services, working with national and international clients, private and public sector organisations, assisting in strategic risk management and the meeting of security needs. I bring extensive and deep experience and skills to all the projects I undertake.

I was an active member of the Management Committee for the Information Assurance Advisory Council (www.iaac.org.uk) from May 2002 to March 2011, and led their widely-acclaimed research programme for five years. I am a member of the International Board of Referees for *Computers and Security*, have presented at public conferences on a variety of topics, and contribute articles to recognised journals in the field.

EXAMPLES OF MY EXPERIENCE AND EXPERTISE

The work I undertake tends to fall into the following three broad categories.



- Much of my work involves helping clients use security data to create meaningful results that support risk management decision making. Security data could be threat data, vulnerability data, countermeasure data, compliance data, incident data, staff data, almost any data that clients might gather from within their systems or environments. I use my security experience and data analysis skills to help clients extract the insights buried within their data and build the risk or other indicators they need to support the risk management decisions they want to address.
- The second broad category involves creating innovative solutions to difficult problems, often taking on problems that other consultants who lack my analytical training would not be able to take on. This includes the research work I undertake for clients as well as my own research.
- The rest tends to be on strategic projects for clients who need the very best calibre skills and experience to ensure important projects are delivered correctly or to supplement the breadth, depth or specialist knowledge of their existing security teams.

The following highlights illustrate the scope of my experience.

THE USE OF SECURITY DATA

- The development of threat and risk models.
- Calculating the security added-value of a managed IT service.
- Showing how TBSE could be applied to a wide range of corporate security challenges.
- Developing a new way to assess and present system and operational risk.

INNOVATIVE SOLUTIONS TO DIFFICULT PROBLEMS

- Directing IAAC's People-Centric Information Assurance research.
- Directing IAAC's Identity Assurance research.
- The research for, and full development of, Threat-Based Security Engineering, TBSE.
- The research for, and full development of, a Taxonomy of Threats, Attacks and Incidents.
- A thorough analysis of the security issues raised by breaking the SET paradigm.

STRATEGIC PROJECTS

- The development of a complete suite of information security policies.
- With a partner, researching and writing "The Privacy Dividend" for the UK ICO.
- The assessment of a number of GRC (Governance Risk and Compliance) software products.
- Devising a multi-million pound Security Improvement Programme.
- The development of a security monitoring service model.



- Directing a multi-national team providing eCommerce strategy and implementation assistance.
- Developing a Global Security Framework.
- The development of a Logical Access Control Framework.

PUBLICATIONS AND CONFERENCES

I have presented at conferences on a variety of subjects and written articles for publication in international journals and the press. I have delivered training courses on a wide variety of topics and have presented seminars on risk modelling and network security for the Royal Holloway (University of London) M.Sc. in Information Security.