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

- (Mid 2010 through to Spring 2013) Working with a leading trading firm to develop a threat model and a risk model that helped them identify their key threats and the level of risk they faced arising from within their IT systems and infrastructure. This helped the client build a uniform compliance assessment programme under which they assessed several hundred applications and supporting components.
- (Spring 2013 onwards) A similar but more detailed pair of threat and risk models for a well-known High Street brand.
- (Late 2008 to mid 2009) Working with a SAAS provider to calculate the security added-value that their service provided and to compare that to a competitor's service. The aim was to design an open, fair, side-by-side test of the two services. The security capabilities of each service were quantified based on the proper scientific analysis of an enormous volume of live data. The security risk faced by customers was then quantified in terms of the probability of major security incidents each customer could expect under each service. This was developed into a financial return for the security benefits provided by each service, that could then be balanced against the service fees customers were charged. The work was independently reviewed by the University of London and shown to be a fair test of the two services with risk and financial results calculated correctly.
- (Spring 2006) Working with a Netherlands-based global medical devices company to show how TBSE could be applied to a wide range of corporate security challenges. This feasibility study showed that the TBSE approach can be applied successfully to any area of security risk, including physical security, personnel security, and business continuity as well as to information security and IT security. The study showed the enhanced security risk management capabilities that become possible once one adopts a scientific approach based on a proper understanding of the dynamics of risk. The study also showed how to present the results to executive and senior management by using them to power a multi-level Risk Dashboard.

- (Winter 2004 - Spring 2005) Working with a London-based international bank to develop a new way to assess and present system and operational risk. The bank had a growing body of internally-created data describing each IT system's degree of compliance to the bank's security baseline. This work introduced new analyses of that data to develop fresh insights and form meaningful conclusions about the nature and level of the security risks the bank faced due to compliance shortcomings. This provided senior IT and business management with a clear, intuitive and more mature understanding of the risks they faced, and allowed senior management to make more informed risk and spending decisions.

INNOVATIVE SOLUTIONS TO DIFFICULT PROBLEMS

- (2009 to mid 2011) Directing IAAC's People-Centric Information Assurance research. IAAC brings together public sector policy makers, private sector business leaders, and academics, to work for the development of a safe and secure digital society. Since early 2009, IAAC's research has focussed on addressing strategic issues to do with the concerns and needs people have relating to the ways personal information is used in the public and private sectors. I developed the research programme for IAAC, designed and ran the individual workshops, and developed the thought leadership for which IAAC is acclaimed.
- (2006 through 2008) Directing IAAC's Identity Assurance research. During this period, IAAC's research focussed on developing policy and governance solutions for trustworthy digital identities. IAAC's results applied equally to public sector national identity infrastructures and to private-sector IDM infrastructures. As above, I developed and executed the research programme and developed the thought leadership results. The programme ended with the creation of a concluding report that identified the barriers to Identity Management progress at a national level and laid out a programme for how those barriers could be overcome.
- (Dec 2003) The research for, and full development of, Threat-Based Security Engineering, TBSE. TBSE is a completely new technique for the analytical modelling of security risk. TBSE models the dynamics that underpin the creation of risk and allows analysts to quantify the expected likelihood and characteristics of security breaches directly from the threat exposure and deployed security countermeasures. TBSE is believed to be the first published technique to apply stochastic methods properly to the forecasting of risk, and it opens up a huge range of possibilities. TBSE can be applied successfully to almost any security threat and countermeasure and is not restricted solely to IT security risk. This presents an extremely exciting prospect for the security industry and opens up the prospect of major new advances in the field, including but not limited to solving the problem of how to forecast objectively the benefits of proposed security expenditures.
- (Summer 2003) The research for, and full development of, a Taxonomy of Threats, Attacks and Incidents which allows all attacks, malicious and accidental, internal and external, to be identified for a given system or environment. The taxonomy also exposes where within the risk dynamics individual controls produce their effect so that uncontrolled risk pathways can be identified and addressed.

- (1999) A thorough analysis of the security issues raised by breaking the original SET paradigm (SET - the Visa/MasterCard Secure Electronic Transactions specification on which today's EMV specification is based) and allowing cardholder electronic wallets to be hosted at a remote server rather than on the cardholder's PC. This required a penetrating analysis of the SET Trust Model for both conventional SET and for SET with server-based wallets. The analysis followed on from an earlier comprehensive review I performed looking into the ramifications for all parties in the industry of permitting cardholder certificates to be discretionary rather than mandatory. This work was conducted for Visa International and helped Visa to determine its short term and long term strategy for SET cardholder certificates.

STRATEGIC PROJECTS

- The development of a complete suite of information security policies for a major UK insurance company. This entailed developing a Policy Framework that showed all the security policies the company would need and how they related to each other. Then the development of all those policies (18 in total) plus associated supplements and guidance documents, to a standard format and style so they all had the same look and feel to them and worked together as a set.
- In partnership with Colin Watson of Watson Hall Ltd, researching and writing a report commissioned by the UK Information Commissioner's Office articulating the business case for the protection of privacy. This ICO commission was in response to a finding from a previous report ("Privacy by Design", written by EPG) that identified the lack of a business case as a major reason why organisations did not do a better job of protecting privacy. Central to the report was its ability to provide a clear understanding of the various components of a privacy business case, and the useful tools and checklists that were provided to support organisations developing business cases of their own. This report was launched by the ICO on the 3rd March 2010.
- The assessment of a number of GRC (Governance Risk and Compliance) software products for an international bank. The bank had outgrown its bespoke software system and needed to upgrade to a higher-functionality, fully-supported, commercial product. This work included an initial review of a large number of commercial systems, the development of an RFP, the evaluation of bids, and the development of recommendations. It also included discussions with suppliers around enhancements to their products to support the more advanced aspects of the client's in-house methodology that I had been instrumental in developing.
- Devising a multi-million pound Security Improvement Programme for a global manufacturing company, and directing a team of 6 consultants across a number of projects helping the client implement the programme. The work encompassed 24 specific security improvement activities organised into four main strategic threads: Enterprise Risk Management Approach; Early Warning Systems; Infrastructure Security; Incident Management.
- The development of a security monitoring service model. Information systems security monitoring was to be brought in-house and distributed across a global security team. The service model covered all the activities and tasks involved in running the selected log collection and analysis software, enrolling IT systems under the moni-

toring scheme, analysing the alerts warnings and informational output produced by the monitoring systems, investigating and responding to alerts, and dealing with the security breaches and bad practices brought to light.

- Directing a multi-national team providing eCommerce strategy and implementation assistance to an Oil major. The client was developing an enterprise-wide eCommerce infrastructure built around a PKI and related security frameworks. The team provided diverse assistance across all aspects of the development, to ensure that the resultant infrastructures were efficient and effective, easy for the business to use, interoperable, manageable, and had the versatility to support whatever the business's future priorities might be.
- Developing a Global Security Framework for a London-based international bank. The work began with the development of a new Security Governance Model describing and structuring the set of arrangements put in place by the Managing Board in fulfilment of their security obligations. The security strategy and security framework followed naturally from the governance model and showed in a clear and structured manner how and why the Bank performed the security activities it performed, and where there were misalignments or omissions in need of further development.
- The development of a Logical Access Control Framework for a London-based financial services provider, formalising the activities and the large number of tasks involved in controlling logical access to systems and data, plus providing detailed policy rules for the control of each task.
- The definition of comprehensive security frameworks and strategies for numerous clients including a major UK brand name retailer, a major international bank operating from London, a national Post Office, and a leading Swiss Bank.
- Providing a suite of Voice Security services to assist clients large and small to reduce their PBX vulnerabilities and their risk of telecoms fraud and abuse. The services include audits and security reviews of voice systems, the development of voice security policies, processes and practices, and voice security management.

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.