Information Systems Audit and Control Association

SEPTEMBER ***2004***

The London Chapter Newsletter

PRESIDENT'S COLUMN

Incorporation

At a special meeting on 27 November 2003, members voted in favour of changing the status of ISACA London Chapter (currently it has the legal status of a "club") and to re-constitute it as a company limited by guarantee. The Board has been actively pursuing this and plans are well advanced to have this in place by 1 January 2005, the start of the new financial year. We will be providing members with more details in due course via the Newsletter and website. If you have any questions about this in the meantime, please contact the President or Secretary.

COBIT

The Chapter's next CobiT Training Course is planned for 20 & 21 October 2004. Details are attached and on the website.

A "COBIT Security Baseline" document has been made available for a limited time as a complimentary, member-only download at www.isaca.org/cobitsecuritybaseline. This guide focuses on the specific risks of IT security in a way that is easy to follow and implement for all users; small to medium enterprises, executives and board members of larger organisations as well as home users.

Membership Renewals

Current members will be sent 2005 renewal invoices in early October. If you know of any prospective members wishing to join, you may wish to inform them that as of 1September 2004, 2005 ISACA membership is available. This means that any new member joining ISACA between 1 September and 31 December 2004 will pay the 2005 dues and receive the reminder of 2004 at no charge. New members are encouraged to join online, reducing the new member joining fee from US $30 to USD $10.

Membership Login into ISACA Websites

Members experiencing difficulties logging onto the www.isaca.org site should use the Help link on the Home Page or contact membership@isaca.org or feedback@isaca.org to obtain their login information. Members wishing to log onto the ISACA London Chapter website are reminded the login credentials are as follows: for the members' pages, the userID is 4london and password is 2view. For the Datawatch Online, the userID is 4members and the password is mag2view

CISA and CISM Examination Results

The 2004 CISA and CISM results have been made available to individual candidates, but the Chapter is still awaiting the details. These will be made available on the website as we have these. A reminder to those who passed the CISA exam in 2004, you must register your working experience with International to complete the certification process.

Datawatch Online

The first edition of Datawatch Online appeared at the end of June 2004 and the publications team is hard at work to ensure that the next edition is available before the end of this month. A reminder that we are always looking for new articles, so please get in touch with the Editor if you wish to contribute.

Research

ISACA Head Office has advised that the following research projects are in progress with target release dates for later this year.

- Managing Enterprise Information Integrity: Security, Control and Audit Issues
- Linux Security and Control Features
- Managing Risk in the Wireless LAN Environment: Security, Audit and Control Issues
- Cybercrime: Incident Response and Digital Forensics Services

CHAPTER ADMINISTRATION

Contacting the Chapter

Christine will usually be available between 08.30 - 12.30 each weekday to take telephone calls and answer emails. If she is not available just leave a message on the ansaphone, and she will get back to you as soon as possible. Alternatively you can email her. All her contact details are at the foot of the page. **It is important to register your attendance at our monthly meetings with Christine either via the London Chapter website or by emailing her direct.**

MEMBERS' MEETING 23rd SEPTEMBER
ABN-AMRO, 250 BISHOPSGATE. 5.30PM

Threat-Based Security Engineering **Speaker: Dr. John Leach**

For many years now we have had to live with the fact the information risk management is an art , not a Science. This has been a source of immense frustration to many people, not least to those who have a responsibility to shareholders to ensure that their company's information assets are properly protected as well as properly used. At a deep technical level, there is one underlying problem which we need to solve. It is the problem of how to model risk analytically.

If we could solve this problem we would be able to quantify risk in meaningful numerical terms and forecast reliably how our level of risk would change as we varied our security deployments. This would allow us to calculate how much security benefit we could get from each security measure. We could determine which security measures were most effective and which were of marginal benefit. We could work out objectively how much of each security measure we would need in order to achieve a given level of protection, and could optimise our countermeasures to satisfy our security needs with the minimum of cost or operational impact. We would be able to scale our security measures dynamically to maintain a constant level of protection against an ever-changing threat. If we could solve this risk modelling problem, we could lay the foundation for transforming information risk management into a properly grounded engineering science, leaving behind the frustrations and difficulties inherent in its having remained an art.

Threat-Based Security Engineering (TBSE), takes a whole new approach to risk modelling. It adapts the types of modelling techniques which have been well tried and tested in other disciplines such as econometrics and applies them to modelling information security risk. If it turns out, and we will know

this better once we have more experience doing this, that TBSE gives us a valid and effective solution to this long-standing underlying problem, then the way will be clear for us to develop the tools and techniques need to forecast and manage information security risk in a similar manner to,say, how the Bank of England forecasts and manages inflation. The first results from applying TBSE to specific information security risks are very encouraging. It is still early days but at the moment there appears to be no reason why TBSE couldn't be applied successfully to a wide range of threats and any counter-measures.

This presentation will introduce the TBSE approach, indicate at a general non-technical level how it differs from past unsuccessful risk modelling approaches, and describe some of the capabilities if offer. It will summarise the initial applications to which TBSE has been applied and present an overview of the results and insights which TBSE has already started to provide.

Dr. John Leach

John Leach has been an Information Security professional for over 18 years. His career started in 1986 when he created and managed a small internal IT security team for the NatWest Bank. In 1991 he joined Zergo and rose to become one of the three Principal Consultants who headed up that consultancy team during its most successful years. Since then he has created and headed IT Security consultancy teams for Trusted Information Systems, Network Associates (by its acquisition of TIS), Global Integrity and Predictive Systems (by its acquisition of Global Integrity).

John Leach set up his own independent consultancy in December 2002. His principal areas of expertise are in risk modelling, security improvement programmes, security infrastructures, network security and e-commerce security. He specialises in innovative solutions to complex problems, bringing together his academic research background and his long experience working with commercial organisations. He has worked for clients across most sectors of industry, including Financial Services, Oil and Petrochemicals, Manufacturing, IT and Telecommunications, Civil Government and Defence. He has developed and deliver3ed numerous training courses and workshops for clients and presented at public conferences on a variety of topics, most often on the subjects of risk modelling, electronic commerce security and network security.

FUTURE IT TECHNICAL MEETINGS

28 OCTOBER 2004:	Basel 11. Speaker: Roger Southgate
25 NOVEMBER 2004:	The Work of the National High Tech Crime Unit. Speaker: Tony Neate
16 DECEMBER 2004:	Top 20 Risks Study by the Sans Institute. Speaker: Ross Patel
27 JANUARY 2005:	IT Governance Framework. Speakers: Legal & General Directors
24 FEBRUARY 2005:	Auditing Networks – Routers. Speaker: Phil Pinder
17 MARCH 2005:	Identity Theft in the Corporate Environment. Speaker: Peter Wood
21 APRIL 2005:	Aligning Risk Mitigation Initiatives with Strategic Management Concerns. Speaker: Bob Vyas
26 MAY 2005:	To be Confirmed
23 JUNE 2005:	Data Mining and Visualisation Techniques for Digital and Paper-based Data.