

AJOY GHOSH - SUBJECT COORDINATOR

Ajoy has 12 years' experience in the area of computer crime, IT Security and Privacy. After originally graduating as a Computer Engineer, he spent a number of years investigating computer-related crimes for law enforcement agencies. He then joined Westpac Banking Corporation as an IT Audit Manager and then an Information Security Manager. Ajoy has performed senior consulting roles with Unisys Australia and 90East (Asia-Pacific), during which time he successfully managed delivery of key projects to headline clients.

Ajoy is the author of Standards Australia's Handbook 171: Guidelines on the Management of IT Evidence, advises a number of industry and government committees on information security and cyber-terrorism and is an editorial advisor to media.

DATES AND VENUE

The Commercial Crime course is held several times throughout the year at the Professional Development Centre, Bathurst Campus, Charles Sturt University.

For a list of future course dates and availability please contact the Program Coordinator.

FEES AND CHARGES

This course is fee paying. The fees cover tuition, resource material and any relevant statutory charges, plus accommodation and meals when attending the workshop.

A corporate discount applies if 15 or more people from one organisation participate.

Students will be individually invoiced for the total cost of fees, meals and accommodation before commencement of the course. Participants who pay their own fees may be able to claim a tax deduction, provided the study is relevant to their employment.

Refunds

Refunds will only be made where the request for cancellation is received 10 days prior to commencement of the course, less an administration charge of \$150 per participant. Cancellation occurring after this time will lead to forfeiture of the course fee. Another member of an organisation may be nominated to attend in lieu of forfeiture, however the substitute's name must be supplied to the Program Coordinator at CSU at least two business days prior to the commencement date of the course. Cancellations must be made in writing and it is the responsibility of the participant or his/her organisation to confirm that the written cancellation has been received by the Centre.

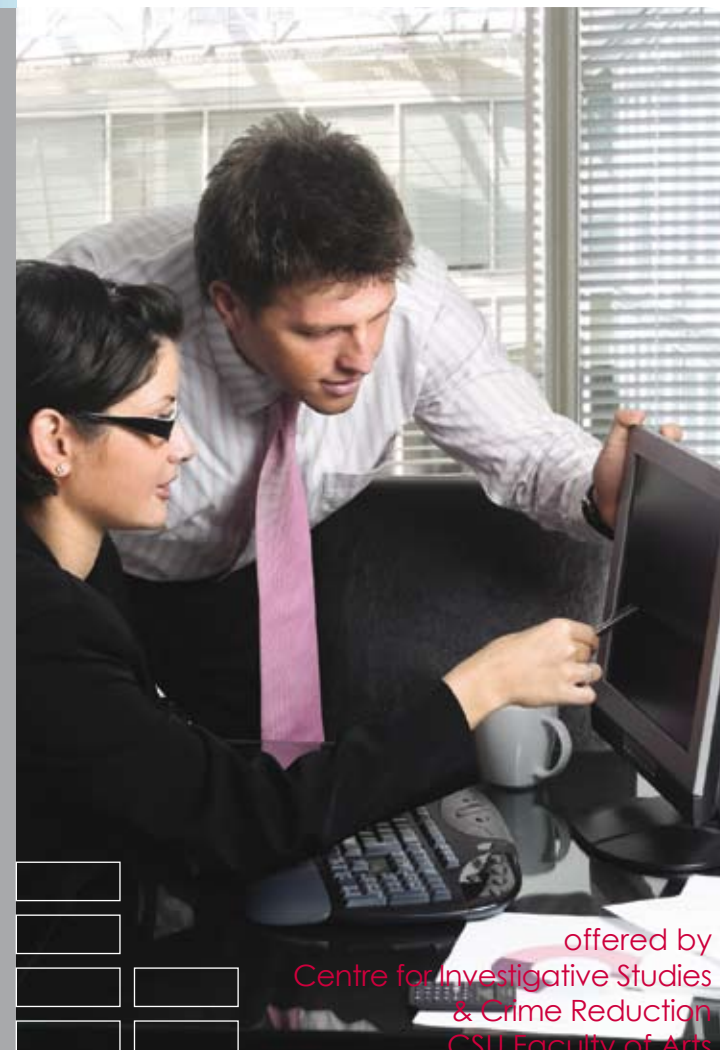
FURTHER INFORMATION

For further information regarding the Centre for Investigative Studies & Crime Reduction or the courses offered through the Centre, visit our website: www.csu.edu.au/special/ciscr or contact the Program Coordinator.

THE WORLD IS CHANGING. GET READY.



A SHORT COURSE IN Investigating eCrime



CONTACTS

For more information contact:

Administrative Assistant
Centre for Investigative Studies & Crime Reduction
Australian Graduate School of Policing
Charles Sturt University
PO Box 168
MANLY NSW 1655

Telephone: 02 9934 4835
Facsimile: 02 9934 4830
Email: ciscrinfo@csu.edu.au

www.csu.edu.au

The Commonwealth Register of Institutions and Courses for Overseas Students (CRICOS) Provider Number is 00005F (NSW) and 01947G (VIC) for Charles Sturt University.
© Charles Sturt University, 2008.

offered by
Centre for Investigative Studies
& Crime Reduction
CSU Faculty of Arts



Investigating eCrime

offered by
Centre for Investigative Studies & Crime Reduction
CSU Faculty of Arts



INTRODUCTION

In adversarial legal systems, information technology evidence is a tool that can be used to protect an organisation by (i) litigating, including criminal prosecution; (ii) defending litigation; and (iii) justifying key decisions to regulators or stakeholders. However, the admissibility of computer records is often questionable. Computer forensics is traditionally viewed as an expensive 'post mortem' exercise that may or may not yield results. However, with some planning, evidence can be discovered, preserved and presented in a cost effective manner. This residential course presents a system lifecycle methodology that maximizes the evidential weighting of electronic records.

COURSE OBJECTIVES

1. Develop an understanding of what criminals do online, why they do it and how
2. Develop an understanding of the variety and efficacy of crimes and victims
3. Develop an understanding of various interventions
4. Basic understanding of electronic evidence and the developing discipline of computer forensics

LEARNING OUTCOMES

On the completion of the course, students will be able to:

1. Profile various types of cybercrimes
2. Choose an appropriate intervention and explain why that particular strategy works
3. Understand the principles of handling electronic evidence and presenting it to a fact finder

COURSE OUTLINE

Day 1

Introduction to eCrime

What is eCrime?

Criminological perspective: Means, motive and opportunity

Developing a profile

Day 2 and 3

Introduction to eLaw

What is eLaw?

Extending traditional law

360 degree perspective: Regulation, civil actions and self protection

Procedural law

Day 4 and 5 – (in computer laboratory)

What is eEvidence?

Evidential best practice

Computer Forensic 101

Presenting eEvidence

Group project (to be completed by Day 5)

Scenario based projects requiring group to develop profile, examining interventions and develop prosecutorial theory including evidential issues.

TAKE-HOME EXAMINATION

Five short essay questions of which three need to be answered. Questions cover all topics and are either theory or practice based.

Upon successful completion of the course, including the take-home examination, students will be awarded the Certificate of Attainment of the University. The Certificate of Attainment may later be used by those who choose to enrol in the University's Graduate Certificate in Fraud Investigation, the Graduate Diploma of Fraud Investigation or the Master of Arts (Fraud Investigation) to claim a one subject credit that will count towards either of these graduate awards.