



# Information Risk and Security

Preventing and Investigating Workplace Computer Crime

Edward Wilding

April 2006  
364 pages  
978-0-566-08685-4

244 x 172 mm  
Hardback  
\$160.00



Information Risk and Security explains the complex and diverse sources of risk for any organization and provides clear guidance and strategies to address these threats before they happen, and to investigate them, if and when they do. Edward Wilding focuses particularly on internal IT risk, workplace crime, and the preservation of evidence, because it is these areas that are generally so mismanaged.

There is advice on:

- preventing computer fraud, IP theft and systems sabotage
- adopting control and security measures that do not hinder business operations but which effectively block criminal access and misuse
- securing information - in both electronic and hard copy form
- understanding and countering the techniques by which employees are subverted or entrapped into giving access to systems and processes
- dealing with catastrophic risk
- best-practice for monitoring and securing office and wireless networks
- responding to attempted extortion and malicious information leaks
- conducting covert operations and forensic investigations
- securing evidence where computer misuse occurs and presenting this evidence in court and much more.

The author's clear and informative style mixes numerous case studies with practical, down-to-earth and easily implemented advice to help everyone with responsibility for this threat to manage it effectively. This is an essential guide for risk and security managers, computer auditors, investigators, IT managers, line managers and non-technical experts; all those who need to understand the threat to workplace computers and information systems.

## Contents

Introduction; Perception of risk; Computer fraud; Espionage, intellectual property theft and leaks; Password misuse; Trash risk; Wireless risks; Sabotage, extortion and blackmail; Social engineering; Risks with personal computers; Pornography; Anonymous letters; Press leaks; Incident response; Ground rules on computer evidence; Covert operations; Analytical modes; Investigative resources; Computer evidence in court; Exit procedures; Conclusion; Appendices; Glossary; Index.

## About the Author

Edward Wilding has investigated several hundred cases of computer fraud and misuse in many jurisdictions. His previous book, *Computer Evidence: A Forensic Investigations Handbook* (Sweet and Maxwell 1996) was one of the first to discuss computer forensic investigations. The author has lectured widely, trained incident response teams, and conducted security and risk reviews for a diversity of clients. He has also served as an expert witness in civil and criminal cases, tribunals and official hearings, including the Hutton Inquiry. In 2002, he co-founded Data Genetics International (DGI), specializing in computer crime investigation, incident response and forensic evidence.

[www.gowerpublishing.com/isbn/9780566086854](http://www.gowerpublishing.com/isbn/9780566086854)

# GOWER

To order this book please visit [www.gowerpublishing.com](http://www.gowerpublishing.com), or email [orders@ashgate.com](mailto:orders@ashgate.com)  
A 10% discount applies to orders placed through [www.gowerpublishing.com](http://www.gowerpublishing.com)