

**SIMON BILES. MBCS. CITP. CISSP. OPSA.
ISO17799 LEAD AUDITOR**

**DIGITAL FORENSIC ANALYST AND INFORMATION
SECURITY SPECIALIST**

P: 0118 979 4043

E: enquiries@forensicequity.com

FORENSIC EXAMINER SINCE: 2002



QUICK NAVIGATION

[1 Areas of expertise](#) | [2 Summary](#) | [3 Experience](#) | [4 Committee memberships](#) |

[5 Notable work](#)

1 AREAS OF EXPERTISE

1.1 Digital forensics

1.1.1 Including: Computer forensics, Information security, Infrastructure and network architecture, Mobile networking.

2 SUMMARY

2.1 Simon Biles is a highly experienced digital forensic analyst and information security specialist with over 12 years' experience in working with Microsoft, UNIX and assorted LAN, WAN and mobile networking products.

2.2 Over his career Simon has obtained significant exposure to infrastructure and network architecture and holds technical skills and architectural expertise across a wide variety of technologies including Cloud (IaaS, PaaS, SaaS), Virtualisation, E-commerce and Social Media.

- 2.3 Simon also has extensive experience of creating policy and procedure to support Information Management, including Disaster Recover (DR), Business Continuity (BC), Security, Incident Response (IR) and Data Protection. He is also certified as a Lead Auditor on ISO 17799, the predecessor to ISO27001, with experience of implementing both standards.
- 2.4 Simon's experience and expertise have been utilised across both private and public institutions including: Banking and finance, software and hardware development, national and international charities, criminal defence, central government and the NHS.

3 EXPERIENCE

- 3.1 Leading computer and digital forensics expert
- 3.2 Leading forensic expert in audit and fraud assessment and in loss prevention.
- 3.3 Vastly experienced across multiple Operating Systems (Windows, Linux, UNIX [most flavours] & MacOS) & Virtualisation (VMWare) and Software (SQL, Oracle, Office, Encryption, Anti-Virus, etc.)
- 3.4 Infrastructure architecture, security architecture and secure system design specialist with technical expertise across a wide variety of technologies including Cloud (IaaS, PaaS, SaaS), Virtualisation, E-commerce and Social Media.
- 3.5 Holds an in-depth knowledge of numerous information management and security standards and best practice guides including – HMG Information Security Standards (IAS1, IS2, JSP440, NHS, CESG Memos, etc.) and Risk Management Accreditation Document Sets (RMADS), ISO 27001, ISO/BS 17799, COBIT and Sarbanes-Oxley Standards.
- 3.6 Highly experienced and respected e-mail, mobile (Blackberry, SmartPhones), satellite and telecommunications expert
- 3.7 Leading defence expert having successfully analysed and reported on numerous cases.

- 3.8 Simon's work includes: finding and retrieving material, copyright and intellectual property theft, breaches of acceptable use policies, data recovery (including the retrieval of deleted data such as email correspondence, address book contacts, calendar entries, internet history and dates and times of key events), user identification, hard drive and server imaging and the securing of volatile data.
- 3.9 All Investigations are undertaken in strict compliance with the Association of Chief Police Officers (ACPO) guidelines for managing and evaluating digital evidence.
- 3.10 Involved in the research and development of new forensic tools and techniques.
- 3.11 Highly accomplished risk, vulnerability and threat assessor.
- 3.12 CISSP Certified (since 2004).
- 3.13 Encryption expert – public key, certificates & secret/shared key, Full Disk Encryption (FDE).
- 3.14 Payment Card Industry (PCI) Data Security Standard (DSS) – audit and compliance expert.
- 3.15 Highly respected policy and procedure development consultant for global organisations.
- 3.16 Teacher and mentor at a postgraduate level: Visiting Lecturer at De Montfort University Cyber Security Centre – Network Forensics & Alternate Operating Systems.
- 3.17 Experienced and qualified trainer in all aspects of digital forensics and information security including: forensic awareness, security awareness, first responder and incident response, security assurance, linux security.

4 COMMITTEE MEMBERSHIPS

4.1 Certified as a Lead Auditor for ISO 17799.

5 NOTABLE WORK

5.1 Author of a number of key publications including:

5.1.1 Building Security and Directory Solutions for UNIX Using the Windows Server 2003.

5.1.2 Active Directory Kerberos and LDAP Services, Microsoft, January 2004.

5.1.3 UNIX and Microsoft Single Sign-on, SysAdmin Magazine, September 2004.

5.1.4 Migrating UNIX Daemons to .Net Services using Visual C++, Microsoft, March 2004.

5.1.5 Several Lessons in the "Hacker High School" Series from ISECOM.

5.1.6 Snort Cookbook, O'Reilly UK, 2005. ISBN: 0596007914.

5.1.7 Hacking Exposed Linux 3rd Edition, Osborne/McGraw-Hill,U.S., ISBN: 0072262575

5.1.8 Technical Reviewer on: Computer Security Basics 2nd Edition, O'Reilly.

5.1.9 Internet Forensics, Robert Jones, O'Reilly.

5.1.10 Regular columnist on Information Security on Forensic Focus.