Mark Schiller BA CISSP

**Mobile: +44 (0)7775 747100**

**E-mail:agency@markschiller.com**

<http://www.linkedin.com/in/mcscissp>

**Key Attributes**

A business orientated security professional with 15 years experience of working at all levels within an organisation as a trusted advisor for information security.

Mark has a long history in security transformation in organisations and capable of operating at a low micro level or at a higher macro enterprise wide levels and the political dynamics which come with this. A full appreciation of the commercial and legal aspects that such projects can bring and how to mitigate these issues.

Mark has direct experience of mentoring CISO’s and providing consultancy acting as a trusted advisor on information security matters for some of the world’s largest organisations.

Mark has acted as an interim CISO for a large number of diverse organisations.

Always use good communication skills and interpersonal skills to achieve excellent results where others have simply failed to gain the trust and business engagement required to deliver effective information security.

Experience of dealing with people either of a technical or non-technical background and explain complex areas of security in a down to earth and easy to understand manner using sound business reasons for justifications and where appropriate highlighting legislative requirements.

A firm believer in management by fact and thus not easily blinded by the latest solution from vendors and a great believer in taking a holistic approach to security. Excellent vendor management skills and the ability to look at delivered value from security investment and manage budgets accordingly.

Enjoys working in culturally diverse organisations and thrives on being evangelical about security and selling security as a business benefit and not the often perceived hindrance to business.

Good experience of off shoring and outsourcing and the effective implementation of security measures required to facilitate the business and ensure an accepted level of risk exposure to the business. Various experience within organisations has ensured a good level of experience in delivering solutions to secure emerging markets for large corporates

SC cleared

**Interim Head of IT Security**

**The Bank of England**

**January 2014 – Present**

Brought on board to drive wide scale change and bring together a new IT security organisation from scratch amalgamating various teams within an organisation whose mission is “promote the good of the people of the United Kingdom by maintaining monetary and financial stability” and is responsible for processing all interbank activity in the UK with a 320 year heritage behind it and with a unique threat profile.

Driving forward aggressive change within the organisation delivering a completely new security structure bringing together teams previously in other areas of the organisation and driving new capabilities in the Bank

Responsible and accountable to a board member for all aspects of IT security delivery and service provision within the Bank of England covering critical national infrastructure, high value payment systems and providing security to highly sensitive economic and regulatory data.

Oversight of all operational security teams within the Bank and specifically engaged to assist with the building of capability of the Bank’s IT security team and to help drive forward an IT security enhancement programme

Responsibility for a team of over 50 people at various stages in their career lifecycle covering security consultancy, threat management, identity and access management, security operations, and a security operations centre.

Assisted with the negotiation of new terms for managed services contracts

Instigated a step change in the capabilities the bank was brining on board in terms of people and identified areas of the organisation which required modernisation or

Responsible for effecting change with key security solutions providers

Effected change in key areas such as continuous improvement in security delivery and implemented a more efficient means of directing security resources.

Key member of Security programme board specifically tasked with providing a sanity check on initiatives given previous experience at other organisations in the commercial sector, helped drive the mission statement for the programme and ensure best value is obtained from what it was delivering.

Attended external meetings representing the Bank as a service provider to various payment schemes and stakeholders fielding questions as required on the Bank’s security posture.

Personally oversaw the recruitment and selection of key hires ensuring that the people hired met the requirements for the long term future of the organisation

Providing briefing notes to the senior members of the Bank’s Court (executive body) on IT security issues to ensure they were best equipped to deal with any security topics that may be in the media

**Interim Deputy CISO for Prudential UK**

**Computacenter**

**May 2013 – December 2013**

Mark was tasked in this security leadership role with providing services to FTSE 100 life and pensions organisation acting as interim deputy ciso and providing the organisation with consultancy on a day to day basis in relation to security strategy and security transformation.

Mark also for this client acted as the interim CISO and deputy CISO as required taking over the team for a number of weeks at no notice and ensuring that the department continued to run smoothly and meet its business objectives.

Mark was also tasked with building out an entire information security consulting practice team for a financial services organisation including running a recruitment and selection process for 12 individual roles and conducting some 105 interviews to aid the client in selecting the right talent for their organisation’s needs and goals and ensuring those permanent hires were capable of delivering the vision and strategy for the organisation.

Carried out a full analysis of the previously ‘big 4’ consultancy proposed target operating model. Assessed fitness of that TOM for the organisation and made a real world sense check on the recommendations. Advised organisation on next steps for implementation and gaps from the boilerplate model supplied by the consultancy. Acted as filter for future consulting engagements to ensure true value was delivered as part of these engagements in terms of practical application of recommendations and relevancy to the organisation.

Mark also was responsible for designing from scratch a cyber-readiness scenario which was designed to test end to end the client’s incident management capability including mobilising C level executives to deal with a fictitious crisis engineered using Mark’s experience.

Wrote from scratch a draft for socialisation of an information security strategy to enable the organisation to have a level of vision for what it was attempting to achieve for information security.

Liaison with 2nd and 3rd lines of defence as required. Drove forward a number of audit actions to closure.

Acting as a trusted advisor on information security and information security strategy and tasked with assisting the senior leadership team with helping them drive forward their security initiatives to completion.

Day to day liaison with C level stakeholders and mentoring of senior employees.

Line manager of staff as required. Development of junior members of staff.

Security Cleared to SC.

**Principal information Security Consultant /Interim deputy CISO Jaguar Land Rover / Various**

**Security and governance consulting practice**

**Integralis (An NTT Company)**

**March 2012 – April 2013**

Engaged at a senior level by Integralis to assist in a security programme of change for one of its largest clients in the manufacturing sector (Jaguar) and undertake activities on a number of other accounts as well

Tasked with advising the client’s under resourced security team on security governance and defining the requirements from ground zero to set up a security governance framework for this large global manufacturing company.

As part of this engagement I was providing industry expertise to the client into automotive information security following my previous experience within this very complex market sector and providing advice on best practices when doing business in new emerging markets in Asia.

Part of this role is to baseline current security capabilities against best practice, various ISO standards and their industry peers to provide an AS IS overview of their security capability and maturity and provide out of that analysis an outline for a security target operating model (TOM) and to gain traction for the security programme providing the impetus and maintaining the momentum of that programme of work.

Designed and led a series of fact finding workshops with 12 different stakeholder groups each with their own view on the organisation and its requirements for the security target operating model (TOM)

A key another facet of the role was providing day to day information security consultancy as required for this client on a number of topics and generally responsible with the account management team for ensuring good communication and relationships with all senior stakeholders on the engagement.

The engagement has very much been taking the organisation through a security evolution following its divestment from a large multinational “mega corporation” to global business in its own right but with little security maturity in place prior to engagement.

The engagement also consisted of advising a client on how to manage the security risks of doing business in emerging markets such as china and brazil whilst maintaining a level of protection in intellectual property.

Advised client on key deliverables as part of a supplier assurance programme and advised clients on appropriate means to manage the security aspects of an outsourcing deal covering their entire IT services department by means of using contractual and technical methods to manage security risk.

Asked to assist a client with a PCI project in the final stages to ensure that some key priority 1-3 deliverables were delivered prior to attestation for SAQ D

Deputised for client CISO’s as required.

**Security Transformation Head – Aviva Transformation Programme**

**HP Enterprise Security Ltd**

**March 2011 – March 2012**

Brought in by HP to provide security leadership, consultancy, governance and best practice on and to head up the large financial services account transformation programme in the insurance sector with a total contract value in excess of $1BN.

Responsible and accountable for ensuring that HPs delivery on this expansive programme meets HP’s contractual obligations on this top 20 contract value financial services reference account.

Was a member of the programme change board with overall responsibility for security governance across the programme and the 80 inflight projects that were in progress at the time of engagement.

Specific responsibility for providing security consultancy and governance for the transformation element of this contract working (as a peer) alongside the programme director, programme managers and project managers to ensure an acceptable level of security and commercial risk to the customer and HP with a wide and varied technology stack including mainframes, midrange and legacy operating systems.

Delivered a portfolio of security projects delivering into the account security projects covering SIEM, technical security tools and business change with a total contract value in excess of £5.5M

Responsible for identifying commercial opportunities on the account for security and have been responsible for various upsells on the account with a value in excess of £5M.

Providing management information in relation to project risks, assumptions, dependencies issues and opportunities and responsible as the sponsor for a number of projects ensuring that these projects have an appropriate direction.

As part of my governance role I was responsible for carrying out gap analysis of the current transformed estate against contractual requirements for security and for commissioning projects as required to cover gaps and working with the customer to obtain interim waivers/exceptions to cover gaps and thus mapping out the As Is state of the programme in order to drive any remediation activities required.

Attendee at a senior level governance meeting with the customer responsible for providing security guidance to that steering meeting on behalf of the HP transformation programme.

Had management responsibility of a project manager and technical authority and general responsibility for their strategy and direction in terms of their deliverables for the transformation programme.

Attended monthly customer facing meetings at director level and was responsible and accountable to that meeting for transformation activities and security for HP.

**Principal Information Security Consultant**

**Integralis – United Utilities PLC**

**September 2010 – March 2011**

Engaged by Integralis following a personal recommendation to assist as a senior consultant on site as part of the Information Security and Governance risk and compliance practice to assist a large UK based FTSE-100 with CNI responsibilities achieve a number of key organisational goals.

These goals including PCI-DSS compliance for its call centre operation; insource all of its IT operations including security operations and establish a new information security practice following a TUPE transfer of staff to the client from their supplier; All within 6 months.

Part of the engagement was to provide both operational and strategic advice directly at CISO and director level on best practices, provide strategic guidance on information security priorities, and provide assurance services to highlight areas of risk previously not disclosed by the outgoing supplier. Wrote a number of 100 day plans for the newly established security team outlining the initial goals of that newly established team.

I carried out a full capability and maturity analysis of the current security structure and assisted the current CISO with putting an appropriate structure in place for an information security department based on my experiences.

I have carried out a full value analysis of their security toolset and assessed its fitness for purpose and highlighted areas for improvement and areas that have not been addressed and fed security requirements into the overall target operating model (TOM) which was being designed at the time.

Assisted CISO in carrying out a skills analysis of the security team and fed this into the new organisational structure which I assisted in the overall design of and assisted the CISO in obtaining board level approval for this new structure.

Delivered a redesigned organisational strategy for its juniper STRM SIEM solution, assisted with the definition of goals for Netwitness and put process around the technology investments in these areas to ensure that security outcomes were consistent and relevant to the organisation.'

Refreshed supplier relationships between the client and vendors and assisted the client in maximising its security investments by ensuring technology was backed by appropriate levels of process and documentation. Obtained senior level assistance from vendors such as Sophos an Juniper

As part of the client’s PCI DSS compliance, I assisted the CISO in designing an appropriate set of compensating controls for the Cardholder Data environment and provided the necessary support alongside an Integralis QSA to obtain sign off from Barclaycard.

Lead the organisation’s incident response function due to a skills gap, mentored the clients staff on best practices, re-wrote the organisation’s cert process and

Re-invigorated that process within the organisation.

Designed a series of tactical plans for the organisation to address key security issues and align short term security deliverables with long term strategic objectives.

**Deputy CISO**

**Volkswagen Group United Kingdom Ltd**

**June 2006 – July 2010**

Engaged to act as the Deputy CISO for all of Volkswagen group's multi billion pound businesses in the UK in this high profile senior level position with a remit covering the full range of business activities including fleet, aftersales, marketing, customer contact and roadside assistance and responsible for ensuring these services were complaint with security best practices, architectural practices and legal requirements. Gained in depth experience of the various processes in an automotive business and the value that security can add as part of those processes.

Drove forward and defined various strategic initiatives including the re-definition of the internal network security model, the complete overhaul of security infrastructure, mcafee endpoint encryption for all clients, an estate wide update of anti-virus software, a completely overhauled vulnerability management process including a regular patch release schedule, and a fresh approach to integrate security considerations into IT projects

Directly tasked with resolving relationships with business areas previously considered unapproachable. Re-established broken vendor relationships and ensured that VWG received the full benefit of its security investment.

Responsible for improving the profile of information security by introducing a range of awareness strategies and by ensuring the group's policies reflected best security practices. These measures included security briefings directly at board level, various awareness campaigns and board level sponsorship of key initiatives. This is now being considered at a global level as a potential approach for areas outside of Germany.

Introduced standards for web application security which were deployed on some of the largest automotive websites in the UK without any impact to business and without loss of service.

Responsible for the implementation of processes to ensure that security was engineered by design and not as an afterthought by pursing a model with the group projects team to ensure that security advice is sought at the outset of projects and with various quality gates implemented overall security governance is assured throughout the design and implementation phases of a project.

Acting as the primary security resource in relation to the off shoring and outsourcing of business critical business functions to Tata Consulting Responsible for ensuring the security controls and overall strategy that were specified as part of the design were implemented correctly by the suppliers concerned and that they were fit for purpose.

Key achievements were to reduce audit findings by 600% and completely turn around the relationship with the business in terms of information security with other IS departments attempting to mirror our achievements.

Trusted Advisor to legal team and Volkswagen UK board as required on information security issues and brought in to deal with various issues of a sensitive nature including criminal and civil investigations.

**Senior Information Security Consultant**

**Reuters Ltd**

**London**

**June 2005 - June 2006**

Working as the senior resource on one of Reuters historically most ambitious security transformation projects, delivering a massive programme of change in relation to their security infrastructure.

**Senior Information Security Consultant**

**Banc of America SA / Bank of America Ltd**

**April 2004 – June 2005**

Lead the technical evaluation and strategic analysis of the EMEA firewall provision, suggested ways in which BOA could capitalise upon vendor relationships and evaluated firewall solutions as potential replacements for end of life equipment. Devised strategic evaluation criteria for the bank to evaluate each platform against a business orientated model. Widely accredited with introducing nokia firewalls onto the bank America estate delivering a sea change in terms of cost and functionality.

Devised a firewall total cost of ownership model for use within the entire bank globally.

**Senior Security Consultant**

**Cable and Wireless Plc / Aviva plc**

**November 2003 - April 2004**

Working as a senior security consultant for C+W as a trusted 3rd party supplier to Aviva plc (Norwich Union Insurance) on the entire global security infrastructure for one of the largest insurers in the UK (Norwich Union).

**Network Security Consultant**

**Norfolk Police Constabulary**

**August 2003 – November 2003**

Role details restricted.

*.*

**December 2002 – August 2003**

**Travelling around Australia and Europe**

**Senior Security Architect**

**Schlumberger Sema Plc**

**April 2002- December 2002**

Senior member of a team responsible for integrating the Schlumberger and Sema global networks providing security analysis and consultancy services to enable the secure migration of services from Sema to Schlumberger.

**BT Ignite Solutions**

**Global Operations**

**E-Business Solutions**

**Apsley**

**April 2000 –April 2002**

Security consultancy for multiple clients including an intercontinental VPN, a defence grade network, a major insurance provider and part of the delivery team for major clients..

**Lead Technical Consultant and Senior Technologies Analyst**

**Sema Group plc**

**Jan 1999 to Jan 2000**

Supervision of staff and management of resources and acting as a technical reference point to team members and deputising for programme manager as and when required and managing own resources including staff, equipment and logistical arrangements and planning.