KPMG

Overview of the i-4 programme

www.i4online.com

—

August 2019

Contents

1. What is i-4?

Keeping members at the forefront of information security

- Founded in 1986 by Donn Parker of the Stanford Research Institute International, the International Information Integrity Institute (i-4) was the first knowledge and experience sharing forum for senior information security leaders. i-4 is the leading forum for security leaders involved in implementing sophisticated risk management and security operations, many of whom hold the highest ranking positions within some of the most influential global organisations.
- i-4 brings together some of the leading minds in the world of information security and risk to help its Members stay one step ahead of the big issues. It is at the forefront of the information security industry, pushing the boundaries on thought leadership, collaboration and innovation.
- The fundamental ethos of the i-4 concept is trust, collaboration, participation, contribution and the willingness to share not only the extensive experience of its membership community but also their valuable intellectual property.
- i-4 is a global forum with a difference, enabling Members to tap into the latest thinking and anticipate emerging trends before they can impact their organisations. Members are able to separate the facts from the scare stories and get more from their investment in security.
- Today's security leaders face an ever-widening range of challenges that are very much part of the top table agenda. i-4 membership helps its Members give the Board and senior management greater assurance that valuable data is protected in a cost-effective way.

> I really enjoyed the range of presentations at i-4 as they challenged my thinking and showed me what's possible.
>
> i-4 Member, Forum 96, February 2019

2. Overview of i-4 member programme

Forums

These three-day events take place three times a year, one each on the west and east coasts of North America, and a third in Europe. The emphasis is very much upon learning, sharing knowledge and solving real problems by interacting with other Members, relevant guests and external specialist contributors.

Regional meetings and roundtables

These member driven events are held several times a year, one-day Regional and half day Roundtables allow Members to focus on one or two specific issues in considerably greater detail, in some cases following up queries and discussions raised in Forums.

Webinars

Members may not always have the time to attend events in person, so i-4's webinars offer an ideal way to keep abreast of important and emerging security issues.

Member queries

If a Member organisation is struggling to overcome a particular challenge, it can readily tap into the collective power of the i-4 membership. Responses to a query are analysed, collated and then published to the Member raising the query and to the broader membership – all Members thereby quickly benefiting from the collective knowledge and experience of the group. See Appendix 1 for a summary recent queries that allow Members to promptly answer the question, 'what is everyone else doing?'

Threat and intelligence exchange

This community provides Members with the opportunity to openly discuss threat and intel information currently on their agenda and explore threats, incidents and other intelligence that people are seeing and would like to explore with other Members.

This monthly cross-sector interactive, facilitated, teleconference underlines the fact that i-4 is all about the sharing of real experience and knowledge and getting on to the front foot with the ever changing challenges facing the world of information security. A monthly opportunity for all Members to air, share and collectively address a challenge, all underpinned by the powerful ethos of openness and sharing that runs through all i-4 activities.

i-4 website – www.i4online.com

All i-4 content, including, Forum presentations, recorded webinars, results of Member queries are all made available to i-4 Members in the private section of the website. A huge repository of many years of valuable intellectual property, covering all aspects of information security from strategic to tactical, from technical to people and all points in between but linked together to provide Members with the information and knowledge they need to stay one step ahead.

> Having been a Member of i-4 for over 10 years I truly appreciate the value membership brings to an organisation, the ability to gain insights and share experiences, even if it is to simply confirm that we're all in the same boat, is invaluable.
>
> i-4 Member, Forum 89, October 2016

3. i-4 differentiators

A highly experienced team

Two of the i-4 Team Members have backgrounds as, CIOs, CISOs and CSOs of complex global organisations and many years' experience in senior security roles. Each of them brings a different perspective to i-4. This is a much greater depth than the competing programmes – this means that i-4 provides a close match to the needs of senior security leaders in the following ways:

- Programme content and deliverables are of a high standard and focused on meeting the needs of senior executives.
- We are able to attract membership and participation from higher calibre individuals, giving attendance at i-4 events a greater value.
- The experienced perspective means that our horizon scanning is conducted through the lens of pragmatic experience – keeping it grounded to implementable improvements in the short and medium term, while at the same time identifying future issues in advance and equipping the Members with front foot knowledge.

Trust and intimacy

One of the firm foundations of the i-4 Programme is an operating model and culture that encourages trust between the Members. While this is backed by an NDA, the degree of trust that i-4 operates under is unprecedented compared to its competitors. This means that participants are much more willing and able to 'tell it like it is'.

During i-4 meetings the relationship building is as important as the content itself – we strive to create an environment where business friendships are made and built. Most Members should leave a meeting having made at least two good connections with peers that will help to solve common problems in the short and long-term.

Focus on larger more complex organisations

Many of the other providers' services are targeted at a wide range of customers, meaning that the content delivered trends towards the lowest common denominator. Because i-4 focuses on the needs of senior executives at large and complex organisations the output covers the issues that challenge these organisations – we see the 'basics' as being covered by other knowledge sharing organisations.

The current membership ranges from some of the world's largest financial services, oil and gas, pharmaceuticals, engineering, telecommunications, healthcare, technology and services companies. While a small number of these also participate in other organisations the biggest players are increasingly choosing to go with i-4 as their sole choice.

Backing by KPMG

In addition to establishing a highly experienced team, KPMG is investing heavily in i-4:

- Taking the quality of content and deliverables to a higher level than provided by our competitors.
- Driving the growth in the number and quality of membership.
- Using KPMG specialists to contribute content and experience and do 'heavy lifting' on behalf of Members.

> The Forum presentations were a fascinating journey and show the potential future state. I'll be using the key takeaways I'm sure.
>
> i-4 Member, Forum 97, February 2019

Appendices

i - Twelve months of i-4 activities

Forums

Forum 97 The Hague 24-26 June 2019

— Our opening keynote speaker, EMEA Chief Security Advisor for an operation system producer opened the Forum with insights into the future direction of artificial intelligence and machine learning. She advocated policies that instilled robust ethical practices alongside the technological advancements business can take advantage of today.

— The Chief Control Officer for a global bank spoke about their approach to Cyber Risk Quantification and how corporations can provide tangible business explanations of their cyber risk exposure and this enable a focussed investment programme demonstrating return on investment.

— i-4 Members enjoyed a presentation from a Director of Policy, Capability and Engagement from a national banking group. This presentation, entitled 'Remaining Resilient in a Changing Threat Environment' focussed on their holistic approach to cyber security through people property and supply chain.

— The Head of Incident Management, Monitoring, Forensics and E-Discovery from a global oil and gas producer presented on how to protect your cloud infrastructure and respond to incidents and avoid Business Email Compromise BEC.

— Senior Security Architect from a global pharmaceutical producer gave a detailed case study presentation on their desktop modernisation project and their adoption of cloud security technologies.

— Attendees then enjoyed a presentation from Europol's No more Ransom Project detailing their mission to protect industry and individuals from cryptographic malware. They shared their Top Tips for industry and gave examples of successful industry collaboration.

— Our closing Keynote speaker, a globally renowned security VP, shared insights of the risk posed by modern malware than can affect enterprise, SCADA and IIoT systems. The case study gave 'real-world' examples or modern attacks and how to effectively remediate them.

— Day two began with a deep dive into Third Party Risk Management, with joint i-4 and Royal Holloway University research and a cross sector benchmarking exercise. This was followed by two industry experts sharing their strategies to combat the risks poses by a complex supplier eco-system.

— 'Security in the Age of Agile and DevOps' gave our attendees valuable insights into how to adapt security functions within a highly efficient code building pipeline.

Our Popular 'Birds of a Feather' breakout sessions gave our Members a choice between three engaging topics:

— Taking Third Party Risk Management to the next level.

— Delivering Comprehensive Information Security on a Smaller Scale.

— Designing an Extensible Architecture That Stands The Test of Time.

— Group Chief Privacy Officer from a global oil and gas corporation shared her view on the future relationship with a CISO. A panel session with other global CISOs explored the best working relationships between these two disciplines.

— Our attendees were given the opportunity to question a financial services regulator and find out what the regulator wished CISOs knew prior to an incident.

— On day 3, our attendees enjoyed an immersive cyber attack simulation exercise. They also heard from illuminating speakers about how to optimise cyber threat intelligence strategies and also the future of SOC implementation and management.

Forum 96 Seattle 25-27 February 2019

— Our opening keynote speaker, Senior Vice President of Engineering for a global cloud service provider opened the Forum with insights into the future directions and the importance of building trust in cloud services.

— A CISO from a global food producer shared an honest account of their organisational transformation journey, which has included information security, and resulted in 75% of IS roles to Milan and Barcelona respectively. This has been driven primarily by cost efficiencies, together with a desire to reshape the business.

— This was followed by the Head of Oversight and Assurance at a global insurance provider sharing how they are measuring improvements in their corporate cyber security culture. The presentation gave details on what they wanted to measure and understand it and to use the results to inform their overall 'assurance picture' that is reported to the Board.

— The deputy CSO for an international ISP presented on Building and sustaining a security conversation with your board.

— A CTO shared insights in the strategy and implementation of Zero Trust Networks within global corporations. He shared how Zero Trust can achieve tactical and operational goals and demonstrate how it will not only transform network security, but function as a business enabler by focusing on strategic business objectives.

i - Twelve months of i-4 activities (cont.)

- A CISO from a global bank presented on Managing Cyber Risk and described the elements of their comprehensive cyber strategy leading to a 'best-in-class' cyber risk posture, and how to communicate to key stakeholders, including the board of directors.
- A CISO and VP from a leading cloud services provider shared hard-earned lessons around potential gaps in metrics, benchmarking and security posture with an eye on what the next five to ten years may bring in the cloud security space.
- We took a deep dive into privacy, looking at the effects of GDPR and the new Californian Consumer Privacy Act. The panel session allowed our attendees to ask probing questions and establish the impact to their cyber security strategy.
- We heard an enlightening talk from Head of Security Research and Development at a global networking and security company focussed on the use of AI and ML to track threats from DNS attacks. He shared how effective ML methods applied on global live internet data that leverage anomaly detection, clustering, graph analysis and simple statistics.
- Our third day began with presentations from an operating systems producer and their global CISO giving details of how he engages the board on governance, managing technical debt and future proofing the corporation.
- A senior applied security researcher shared his insights into collecting intelligence from the dark web and criminal forums.
- A general manager of the Risk Management function gave us her insights into the risk management framework and quantitative approach they use to manage their own compliance and risk.
- A Principal Security Program Manager spoke on building an ecosystem of partners. He explained how it is critical for success, sharing how they work globally to make that happen. He shared details of their partnership with other global cloud service providers, international law enforcement and CSERT agencies.
- A SOC and Investigations Manager, spoke on AI Security Incident Response in their Cyber Defence Operations Centre (CDOC). He shared their strategy in aiming to be a 'Cloud First' company for all new project deliveries. Their team is on the front line of defence for responding to any and all security related events for the cloud core infrastructure and 1st party assets running in the cloud. Based out of the Cyber Defence Operation Centre (CDOC), this team is also the front line for all incoming external incident reports involving cloud first and third party incidents. With full 24x7 coverage and resources in India and the United Kingdom this allows for quick triage, investigation and mitigation of events and external reports.

Forum 95 Montreal 15-17 October 2018

- Our keynote speaker, Assistant Deputy Minister of Operations, Canadian Centre for Cyber Security opened the Forum with his presentation on Building the Canadian Response to Cyber Threats. He described the current cyber threat actors and motivations, then spoke about supply chain challenges.
- He described several pillars or components that underpin this philosophy and how each requires considerable effort in order to develop and maintain trust. He went on to answer questions from the audience, sharing insights into Canada's latest approach and ambitions.
- A global CISO with a telecoms provider shared how his team are handling the automation of patch/vulnerability management. His candid presentation gave details of their strategy to automate asset discovery and management, vulnerability identification, prioritisation by asset risk and automation of patch deployment.
- A Chief Product Officer gave a valuable horizon scan for IoT security for the next 10 years. He gave insights and predictions into the impact on IIoT and cryptography from the emergence of quantum computing.
- A CISO and Senior Technical Manager from an academic institute presented on 'Emerging research in IoT security, privacy and resilience'. They also described a related, collaborative effort with the U.S. Defense Advanced Research Projects Agency (DARPA) to create new technologies in TRacking and Analysis of Causality at Enterprise level (TRACE) to quickly detect and contain advanced persistent threats (APTs).
- A security architect addressed the Forum on the fragility of AI systems. He also discussed some of the reasons why these vulnerabilities occur, along with practical mitigations where available.
- Our 'Birds of a Feather' session topics included: Building an Insider Threat Management programme; Consumer Identity and Access Management; Vulnerability and Patch Management Benchmarking exercise.
- A principle security engineer from a global security /networking company presented on the emerging security issues associated with the new 5G network.
- A director from a leading operating system/software producer presented on how best to prepare for a cyber attack and reduce the negative impact on your brand reputation.
- We turned out attention to cyber insurance, hearing from both specialist brokers and underwriters in cyber insurance who presented on the real-life experiences of buying and claiming on cyber insurance policies.

i - Twelve months of i-4 activities (cont.)

Regional meetings and roundtables

Optimising Cyber Threat Intelligence for global corporations

23 July 2019

Security incidents have become harder to detect, mostly because of the increase in malware complexity and variety. Many i-4 Members already utilise cyber threat intelligence within their network defence operations, yet optimising the benefits CTI can provide remains elusive to many corporations. During two highly interactive discussion sessions we examined the following objectives:

— Ensuring successful automation of threat intelligence using a TIP or other tools.

— Strategic threat assessment and prediction of Black Swans.

— Effective and timely intelligence sharing between different sectors.

— Effective intelligence sharing with suppliers and third parties.

— Leveraging the Mitre ATT&CK framework and its uses.

— Increase in Number Porting Fraud threat from Text to Switch.

Vulnerability disclosure and bug bounty roundtable

8 May 2019

A Bug Bounty Program is a crowdsourced initiative that rewards individuals for independently discovering and reporting software bugs in an organisation's internet-connected assets and applications.

The focus of the roundtable was to understand best practices of vulnerability disclosure and bug bounty programs, as well as key risks running such programs, limitations, use cases and practical lessons learned or highlights from organisations who have a program already in place.

— How should you define and publish your disclosure policy?

— Should you build your own bug bounty program or outsource to a third party managed service?

— How do bug bounties fit within a traditional security assessment model?

Best practices in identity access management

20 March 2019

The i-4 community joined together to explore and share the challenges, current thinking and effective solutions to Identify Access Management. We took a deep dive into the methods of business process implementation as well as discussing some of the tools available. We focussed on:

— How can effective IAM be entrenched in both policy and technology?

— How do you advance your overall corporate security posture when managing multiple identity systems?

Incident preparation, management and recovery

4 February 2019

The i-4 community heard from industry leading experts on how best to prepare, how best to manage and how to recover quickly from a cyber security event.

The event began with a 'live attack simulation' on a network and cloud infrastructure from a hacker's perspective, courtesy of Pen Test Partners. This was followed by Member's discussion on the best methods to identify and thwart an attack before the threat actors cause financial and reputational damage, in particular those incidents that result in media and regulatory scrutiny.

The attendees shared lessons learned from their own events and were able to question the assembled 'subject matter experts' to identify improvements to their current strategies.

Delivering secure development with agile

13 September 2018

i-4 and a global gaming corporation held a knowledge sharing Roundtable event to explore the risks and rewards associated with moving a large corporation to Agile development methodology.

Our participants were all at different stages of adopting Agile and shared their challenges and solutions with the other attendees. We discussed:

— What guard rails are necessary to maintain security within the development lifecycle?

— How do regulators and auditors view the move to Agile and can they be an asset?

— How to engage the board and c-suite on the journey to Agile?

i - Twelve months of i-4 activities (cont.)

Webinars

Building cyber security for people, not machines

Data loss events have many causes. Some are as a result of malicious actors, but the risk posed by negligent or inadvertent data exfiltration via email is arguably far more of a clear and present danger for CISOs and senior cyber security strategists to tackle.

All employees are key decision makers in the enterprise and regularly handle sensitive information on a daily basis yet there are few solutions to identify and stop 'human errors' before harm is caused and reportable events occur.

For the first time, machine learning can understand the human layer, and this i-4 webinar will provide insights into how the industry is beginning to provide global corporations with additional protection.

Tackling child sexual exploitation on corporate networks

This webinar will look at what needs to be applied by different sectors and businesses to effectively fight the spread of child sexual abuse material on a national level. It will also look at how academic research plays an important role in ensuring that law enforcement and other stakeholders, working to combat abuse and exploitation, make well-founded, evidence-led decisions in policy and practice.

Identity crisis

How can you spot a fraudster? As the marketplace for stolen credentials becomes saturated after every data breach, the risk of fraudulent account takeovers and unwarranted access grows. This webinar looks at the science behind user behavioural analysis to provide automation in identifying the criminals at work.

Social engineering

The 'Human Factor' in business process if frequently seen as the weakest link in the security chain and the hardest element to 'patch'.

This webinar from one of the UK's foremost authorities on social engineering tactics gives us the knowledge of the tell-tell signs and attack vectors used most commonly by fraudsters and cyber criminals

Buying cyber risk insurance to support your information protection program

The webinar discussed the significant increase of global attacks and cyber events which requires us to look at a balanced approach (Prevent, Detect, Respond and Predict). Risk transfer represents a key to protecting our information element of the 'respond' area. Cyber cover has become one of the fastest growing areas in the insurance industry today; however, its evolving ever so quickly due to limited actuarial data and changing threats.

Insider threat assessment

A Member presentation on Insider Threats from an expert threat intelligence provider, describing the risk posed to organisations and real world encounters of physical, reputational, privacy and financial risk. The presenter described recommendations to ensure Red Flag employees are identified and monitored correctly.

Cyber insurance – An overview

The presentation provided an overview of how cyber insurance has evolved over the last few decades and the types of risk transfer solutions now available. There was a discussion on how cyber risk quantification and the challenges it represents sit in contrast to more traditional risk areas. The presentation concluded with a summary of what you may consider purchasing cyber insurance for and the mechanics of the purchase process.

Blockchain and cryptocurrencies: The risk and the regulator

The number of individuals and companies utilising and investing in distributed ledger technology (blockchain) and cryptocurrencies is proliferating. The technology is varied and often highly innovative, however, the risks are high and rapidly evolving, as illustrated by the increase in mining attacks, malware and regulation within the sector. In this webinar we explored the risks and potential safeguards associated with aspects of fraud, cybercrime, money laundering and terrorism financing.

UBA: Our journey behind the jargon

The presenter shared a very informative 12 month proof on concept on the application of a User Behaviour Analytics (UBA) tool at a global organisation to address Insider Threat. This well attended and interactive session identified legal and technical implementation challenges and offered predictions for the future.

Updating cryptographic protocols in critical financial systems

The presenter described the process of updating and increasing cryptographic complexity in the face of technological advancements; discussing PKI, RSA and SHA algorithms, their selection and the organisations work with academia to gain assurance on current and future implementations.

One insecure IoT device is a nuisance, an army of them could be our doom

This webinar discussed the growing threat of unmanaged operational technology, common application security flaws in IoT, and hardware security issues, together with mitigation advice and controls.

i - Twelve months of i-4 activities (cont.)

Member queries

3 line of defence – A review

Many i-4 Members operate a 3 lines of defence model. This query aimed to review the scope, roles and accountability of the model and its implementation. In trying to clearly articulate the roles and accountability in a group wide document we have found some activity in the organisation that challenges the model.

This member survey is an ask for members to help i-4 understand how they approach and implement 3LOD and the position and accountability of the CISO/CSO within the organisation and the 3LOD model.

Corporate use of mobile messaging apps, such as WhatsApp, Telegram and Signal

A global insurance provider wished to benchmark their use of messaging apps and the security challenges posed by the use of such technologies.

— Have you identified any legal concerns regarding the traceability of message content?

— Do you currently, or have plans to monitor and or log the content of these apps?

Security policy compliance

As part of a security compliance study, an i-4 Member wished to investigate how fellow organisations ensure their systems, networks, services or products are designed securely and subsequently how security compliance is maintained throughout the life cycle of systems, networks, services or products.

— How do you provide information assurance and risk assessment into the infrastructure and software architectural and design processes?

— How do you manage non-compliance or exemptions to security policies?

Vulnerability management

An i-4 Member reviewed options to more effectively manage vulnerabilities based on risk.

Challenges addressed included:

— Automated patching does not always address the identified vulnerability.

— No integration between vulnerability management solution and the service ticketing system or the system software management solution.

— Priority is based on base CVSS score without environmental factors or system criticality.

— Workstation vulnerabilities are not being remediated within required timeline.

Securing DevOps

An i-4 Member sought to understand what organisations are doing in relation to the tooling, environment and controls that companies employ in relation to modern developers/engineers (i.e. those who develop code !!). They want to ensure they have the right up-to-date tools and access for the job, feel challenged and able to work in modern DevOps ways with modern facilities such as Cloud, to ensure attrition is minimised.

They observed tensions between restricting them for security purposes (for example access to internet resources and the tools that can be used) as opposed to allowing them freedom to collaborate and develop code within and without the organisation.

— Do you offer different network connection policies or segregation depending on the user base ?

Global security operating models

An i-4 member in the telecommunications sector wanted to compare their survey the community in respect of how corporations manage their security across international boundaries.

— How many companies adopted the 3LOD model?

— How many CISOs reported directly to the board?

— What security functions are covered by your cyber security department?

— Which functions are devolved to local markets and which are governed centrally?

Getting market best practices for supplier assurance

'Supplier Assurance', sometimes also known as '3rd Party Risk Mgt.' or 'Vendor Risk Mgt.' is understood to provide assurance (from a cyber or information risk perspective) for applications of services that are delivered via a 3rd party supplier. A Member asked how would you ensure that the controls that apply to the 'in-house' situation are still being met when the service is moved outside.

Bring your own devices

An organisation was reviewing its Bring Your Own Device (BYOD) strategy and seeking an understanding of how other companies are approached BYOD.

Low code applications, robotic process automation and mobile solutions

An i-4 Member was interested in views on Low Code Applications, Robotic Process Automation and Mobile Solutions.

ii - The i-4 team

Since December 2009 i-4 has been owned and operated by KPMG, who continue to invest in and develop the programme to meet the changing needs of its Members. Individuals from KPMG serve upon the i-4 leadership team, which can also call on highly experienced specialists from KPMG Member firms around the world, as well as external security analysts and seasoned industry practitioners and leaders.

Kevin Williams

Head of the i-4 Programme

Kevin became Head of i-4 in July 2017 and brought with him more than 25 years of experience in UK cyber law enforcement and cyber security. He started his career with the Metropolitan Police Service, later joining the National Crime Agency, before working in the cyber security commercial and not-for-profit sectors with Team Cymru. In 2008 Kevin was instrumental in the development of national cybercrime capability. He was the lead law enforcement advisor to UK Government for the creation of the cyber response to the London 2012 Olympic Games, for which he received an Assistant Commissioner's commendation. Most recently, Kevin has been assisting the Mayor of London's effort to help small and medium businesses develop their digital defences and growth through the work of the London Digital Security Centre.

Paul Taylor

i-4 Sponsoring Partner

Joining KPMG in the UK as a partner in 2014, Paul is currently working at board level with a number of global retail and investment banks to address their cyber and information protection challenges. Prior to joining KPMG, Paul has led the delivery of some of the most demanding national security programmes in the UK, operating at the very highest levels of government. He is uniquely qualified to understand the evolving threat environment, as well as having an exceptional track record of driving and delivering change in complex organizations. Paul's contribution to the world of science technology was recognised by his election as a Fellow of the Royal Academy of Engineering in 2013.

> What impresses me most when working with fellow security professionals is the level of collaboration and sharing taking place. I regularly find myself overwhelmed with the level of intellect and experience being applied to how we keep systems safe and secure, and the default response of "yeah, I had that problem, this is what I did to solve it or manage it …"
>
> i-4 Member, Forum 96, February 2019

ii - The i-4 team (cont.)

Darren Brind

Events Assistant

Darren Brind joined the KPMG Cyber Security Team in 2016 to support the Head of Sectors together with his direct reports. Experienced in event and project management he has supported the i-4 Team with projects including rebranding and co-chairing Threat Intel Exchange calls and webinars, coordinating member queries and organising Forums, Regional and Roundtable events. Darren continues to enjoy working in Cyber Security and contributing to the success of the i-4 team.

Montana Narrsingh

i-4 Events and Projects Assistant

Montana has been with KPMG since 2013 and has been with i-4 just over two years. Prior to this she was in the Cyber Security Bid and Knowledge Management team. Montana is currently assisting on all aspects of i-4 including risk management, event logistics, and supporting current and potential Members. Montana is a first port of call for any Member support queries.

Marissa Goulding

i-4 Events Manager

Marissa is the i-4 Events Manager and has been with the programme since 1998. Regardless of the question or help needed, for participants in i-4 events she is the point of contact and coordination for speakers, session chairs and – of course – i-4 Members. Marissa's knowledge of i-4 and how to make an event run effectively are central to i-4 Forums and other meetings delivering real value to the i-4 Membership.

Matthew Roach

i-4 Content Manager

Matthew began his career with the Metropolitan Police Service, later joining the Serious and Organised Crime Agency and latterly the National Crime Agency. He led the National Cyber Crime Unit's Tactical Industry Partnerships Team to many operational successes. Additionally, he managed several high profile, sensitive and time-critical cybercrime and data breach incidents. During his 18 years' service, he received commendations from both Crown Court Judges and the Agency's Director-General. More recently, Matthew has managed cybercrime and fraud teams within the telecoms sector and created cyber threat intelligence managed services within the private sector. Operationally, Matthew led investigations into a global ransomware distribution organised crime group, leading to the first seizure of virtual currency by the National Crime Agency. He also led the NCA's operational response to several high profile data breaches within the telecommunications sector.

ii - The i-4 team (cont.)

David Morgan

Senior i-4 Advisor

David is a recognized and respected thought leader in the security and risk management industry with over 25 years experience focusing on information security, fraud prevention, business continuity and physical/personal security. Prior to moving into consultancy and training & development, David held a number of Board level executive roles including Lloyds TSB (Chief Security Officer), ING Group (Global Head of Information Risk Management & CISO) and Barclays (Group IT Risk & Security Director). He has a proven track record in delivering strategic and organizational change within large complex organizations. David has provided strategic consulting services and interim management to a variety of blue chip organizations in Financial Services, Energy, Pharma, Telecoms and High Tech sectors. In addition, he has run numerous leadership development groups and security master classes for large multinational companies. He was an active i-4 Member for many years, having attended his first meeting in 1995. David is also a Director and co-founder of Security Faculty.

Paul Dorey

Senior i-4 Advisor

An acknowledged thought leader in security, Paul has over 25 years of experience as a security and risk executive at Morgan Grenfell/Deutsche Bank, Barclays Bank, and BP. He has received several awards including Chief Security Officer of the Year, IT Security Executive of the Year, and IT Security Hall of Fame. His involvement with i-4 goes back to the late 1980s including a period on the Membership Advisory Committee (MAC). He is a Visiting Professor in Information Security at Royal Holloway, University of London and is a director of CSO Confidential. In addition to his speaking and lecturing activities he helps companies and government departments in building their information security strategies, risk governance and metrics including acting in interim CISO roles and supporting CISOs in developing their functions. He is Chairman of the Internet of Things Security Foundation.

Kevin Williams
Head of i-4

M: +44 (0)7342 067430
E: kevin.williams1@kpmg.co.uk

Marissa Goulding
i-4 Events Manager

M: +44 (0)7768 262727
E: marissa.goulding@kpmg.co.uk

Matthew Roach
i-4 Content Manager

M: +44 (0)7464 900773
E: matthew.roach2@kpmg.co.uk

kpmg.com/uk