KPMG

Overview of the i-4 programme

www.i4online.com

—

May 2020

Contents

1 - What is i-4?

i-4 is the world's longest running strategic cyber security 'think tank' and peer-to-peer knowledge exchange for CISOs and cyber security leaders of global corporations. The fundamental pillars of the i-4 community are trust, collaboration and education.

Our members share their extensive experience and their valuable insight in to how they currently deal with complex and challenging issues in the information security space. All i-4 activities are governed by a member non-disclosure agreement.

i-4 is a global trust group for cyber security leaders to **enrich their knowledge and expertise**.

We enable 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.

It offers the opportunity **to benchmark amongst peer organisations and share threat intelligence** to keep appraised of emerging adversarial trends.

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.

> "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

Calendar of Future i-4 Events

Date	Event	Location
14 April	Threat and Intel Exchange	Teleconference
12 May	Threat and Intel Exchange	Teleconference
14 May	i-4 Virtual Roundtable – Optimising & Securing Office 365	WebEx
9 June	Threat and Intel Exchange	Teleconference
22-24 June	i-4 Global Virtual Roundtable	WebEx
14 July	Threat and Intel Exchange	Teleconference
16 July	i-4 Virtual Regional Meeting	WebEx
11 August	Threat and Intel Exchange	Teleconference
8 September	Threat and Intel Exchange	Teleconference
TBC September	Roundtable	London
6 October	Threat and Intel Exchange	Teleconference
12-14 October	i-4 Forum 100	Athens, Greece
9 November	Threat and Intel Exchange	Teleconference
10-11 November	Roundtable	Bangkok
26 November	i-4 Networking Event	London
8 December	Threat and Intel Exchange	Teleconference
12 January 2021	Threat and Intel Exchange	Teleconference
9 February 2021	Threat and Intel Exchange	Teleconference
15-17 March 2021	i-4 Forum 101	Santa Clara, CA

KPMG

Appendices

i - Twelve months of i-4 activities

Forums

Forum 99 Orlando 9-11 March 2020

— Our opening key note from a Chief Technology Officer presented on **'Messaging-Based Attacks: Past, Present, and Future'.** We looked at the current defenses companies have in place – how our current approaches evolved, and how the threat has changed.

— Our first case study presented on **'Developing Security Empowered People'.** This outlined their strategy and approach and how they are measuring success.

— We heard another case study from a CISO who presented on **'Your Partner in the Trenches –Creating and Maintaining a Strong Partnership with Your Managed Security Service Provider (MSSP)'.**

— A Cyber Threat Intelligence Analyst presented on **'Bestsellers in the Underground Economy: Measuring Malware Popularity by Forum'.**

— The presentation on **Cloud Security** then used experiences of real architectures and security models to outline practical approaches to the unique challenges in cloud solutions.

— We then heard about incident response and red teaming from a Chief Security Officer who presented on **'Red Teaming: Choose how to lose'.**

— Tuesday started with **'Incident Response and Management – Beyond Your Borders'** discussing the need to be on top of your vendor's security capability as much as your own.

— This was followed by the **genesis and evolution of a Member's Offensive Security Red Team.**

— A Think Piece was presented by a member of the i-4 Team on **Expert Witness –Friend or Foe** where he shared his past experiences.

— Our Birds of a Feather Focus Groups tackled **Cyber Risk Assurance – a 2nd line perspective as well as Threat Intelligence – Consuming and utilising TI without the hard work.**

— Tuesday then closed by a session on **'Embracing Neurodiversity at Work'** presented by a Channel Marketing and Inclusion Champion.

— Wednesday started with a session on **'Covid-19 – Examining the impact on cyber security'** where attendees discussed the risks associated with this biological threat.

— We then heard from a Cyber Security Representative on **'Delivering Cybersecurity Prosperity in North America'.**

— Our next speaker presented on the **alignment of security resources in support of business continuity requirements**, equipping CISO's with the right intelligence necessary to make informed risk decisions.

— Our closing keynote was delivered remotely by a global communications provider who presented on **mitigating and responding to ever-evolving cyber threats**

Forum 98 Philadelphia 22-24 October 2019

— Our opening Keynote presented on **'Peeking behind the Curtain: A look at the 'H' in AI and what lies ahead'.** After a decade of mainstream media hype surrounding the abilities of artificial intelligence (AI) to transform business,

— A CISO presented on **Building a comprehensive information security program in a small, high-value, highly-regulated company**. She shared her journey into her first CISO role, the challenges she's faced and the lessons she's learned along the way.

— We heard how a Member on the best strategic direction to enhance, upskill and develop staff and help **bridge the cyber security skills gap** for government and industry.

— In Session 4 on **Collaboration with Law Enforcement** U.S. Secret Service presented on the Secret Service's approach to Operational Success and working with industry.

— The Security MD of a global ISP shared details of the **main trends in security**, key issues and pressures on global infrastructure providers.

— Tuesday started with **Optimizing and Securing Office 365**, presented by a CISO of a global ISP. He shared candidly about challenges 'Keeping Pace with Evolution – The challenge of balancing functionality with security'.

— This was followed by the Global CISO and a Chief Security Architect on '**Doing Business Securely in the Cloud** – How this Member is working to deploy and secure Office 365 across the globe'.

— A Think Piece was presented by Chief Executive Officer, TAG Cyber on Emerging Technology Landscape –**A random walk through Cyber Security.** The i-4 audience enjoyed a fast-paced journey of the practical implications of the most important (and controversial) topics in global cyber security today.

— Another insightful case study from Head of Tech Risk, Banking Member, shared an approach to **formalise the way emerging tech is evaluated**.

— Our Birds of a Feather Focus Groups tackled topics including **Insider Threat, Building a security culture and improving cyber resilience**.

— Director, Cyber Resilient Systems, started the session with a talk entitled '**The evolution of Cyber Resilience**, where are we today?'

— A Chief Technology Officer spoke of **Organisational Metrics in Resilience**. He shared that by institutionalizing Resilience Management you can gain many benefits of a process approach

— In our penultimate 'Think Piece' a Chief Operating Officer shared his strategy entitled **'Get your horse in front of the cart before you create that Cyber Threat Intelligence Program**' Our Member detailed "the" key tool for articulating upward and tracking over time the value of a program - an intelligence requirements program.

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

— We then turned our thoughts **to 'Vulnerability Research and Response: On bug bounties, collaboration with vendors, and reducing risk to customers**. This discussion focused on vulnerability response/vulnerability disclosure/bug bounties and the partnership with security researchers.

— The closing keynote was a leading academic Member and technical director, gave her session entitled **'Bringing it All Together: Practical Applications in Cybersecurity**'. She highlighted the key ideas and themes presented throughout the Forum, focusing on the tangible ways in which the participants can make these ideas operationally relevant for their organizations. She described a vision of cybersecurity to show how simple steps can jumpstart or advance the journey to implement an operational risk management posture that is more aligned with business concerns. Also the value of being part of the extended community that is changing fundamental assumptions related to cybersecurity.

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 .

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

Regional meetings and Roundtables

COVID-19 Virtual Roundtable

24 March 2020

Due to challenges presented by the COVID-19 virus, the i-4 community convened virtually to discuss, compare and share strategic cyber security responses to the current challenges. Members discussed and answered the following questions:

- How are your MFA and VPN solutions impacted?
- What additional threats are your SOCs reporting?
- How are your BC / DR / Pandemic plans withstanding the situation?

This roundtable focused specifically on challenges and threats around remote working, phishing, people, CMT resilience as well as shadow IT and 3rd party supply chain risk. Remote working, phishing and people were seen to be the most pressing concerns.

Zero Trust Networks – Developments and Implementations in 2020 and beyond

6 February 2020

In conjunction with the Foreign and Commonwealth Office, the i-4 community convened to discuss the challenges by Zero Trust Networks. During the session, participants examined and discussed the following:

- Highlighted the potential business pros and cons of Zero Trust Networks.
- Shared experiences in deployment, use cases and discuss the future direction of Zero Trust Networks.
- Discussed how to implement and set up user group profiles.
- Identified the potential role of commercial grade PKI providers in Zero Trust.
- Examined potential architectural patterns.
- Examined detection and reporting of issues, threats, metrics and risk mitigation.

Security Awareness, Behavioural and Cultural Optimisation.

26 November 2019

The Traditional single-stream security awareness campaigns are failing to deliver sustained improvement in corporate security risk reduction and keep pace with the evolving threats from cyber and risk areas. Phishing simulations, training videos and remedial sanctions can all be utilised, but how effective are they long term?

This roundtable explored the latest thinking, current psychological research and strategies employed across the i-4 community helping organisation to challenge traditional thinking and answer the following questions:

- How do global organisations within the i-4 community improve and 'patch' the security behaviours and cultures of their staff?
- How do you measure improvement over time and show a return on investment in this space?
- What are the best tactics to augment phishing simulations to raise awareness, change behaviours and improve overall security culture?

Regional Meeting – Edinburgh 2019

4th September 2019

The i-4 community convened in the historic city of Edinburgh to hear from leading subject matter experts and peer group CISOs on a range of cyber security challenges, including:

- Cyber Resilience for your Organisation and Scotland PLC
- Planning now to harness the business benefits from AI and ML
- Designing a Corporate Immune System – Tackling the Insider Threat
- Google's Approach to Cloud Security – How CISOs can best keep up with securing the evolving functionality
- Measure Twice, Cut Once ... a more scientific approach to defending our digital footprint.
- Will Cyber Security Exist in 2025? – A horizon scan into the future of the industry and what anticipated advances will mean for CISOs.

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.

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

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

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.

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

Member Queries

The use of Prohibited Applications/Software

An i-4 member wished to re-evaluate their current processes to ensure that risk associated with the use of prohibited applications/software is managed effectively.

This included the evaluation of processes and capabilities that block application-specific traffic at the perimeter as well as solutions that detect/remove or more ideally prevent installs of prohibited software.

Measuring Efficiency of Security Capabilities

An i-4 Member sought to benchmark the following practices: identify data assets, ascribe value to them, ensure coverage, and measure their control efficiency. Initiated by their Executive Committee , they wised to understand how they compared.

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.

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.

Matthew Roach

Head of the i-4 Programme

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

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

Darren Brind

i-4 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.

Samar Iqbal

i-4 Events and Projects Assistant

Samar is an analyst within the KPMG Cyber Security Team where she has experience in Cyber Resilience and Information Security. Samar has worked across many different sectors and clients delivering advisory and assurance services, as well as being an ISO 27001 lead auditor. Samar is currently supporting on all aspects of i-4 including risk management, event logistics and supporting current and potential members. Samar is the 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.

Sarah Stanley

i-4 Content Manager

Sarah has 13 years industry experience spanning across trading, commercial & investment banking, financial regulatory services & national infrastructure sectors. This has presented the opportunity to work within many environments from start-up and immature through to mature and complex environments and cyber security needs.

With a record of delivering both technical and non-technical security projects on time to a high standard within a large complex environment on both small and large projects, she is able to understand the differing views of the business, technical staff and IT security; and able to provide an effective balance between requirements and practicality.

This has enabled knowledge and involvement within information security strategy, regulatory frameworks (SOX, DPA, ISO 27001, PCI-DSS), external and internal audits, infrastructure security configuration and controls, third party and projects risk assessment analysis, business impact analysis, threat and vulnerability analysis, security benchmarking and future state modelling, security governance and reporting, hardening security policies procedures and processes , project documentation, and lead investigations into security incidents/breaches

ii - The i-4 team

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/cyber 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 forum in 1995

Paul Dorey

Senior i-4 Advisor

An acknowledged thought leader in security, Paul has over 30 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 also acts as an expert witness in cyber security disputes. He is on the Executive Board of the Internet of Things Security Foundation.

Matthew Roach
Head of i-4

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

Marissa Goulding
i-4 Events Manager

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

Sarah Stanley
i-4 Content Manager

T: +44 (0)7392274197
E: sarah.stanley2@kpmg.co.uk

kpmg.com/uk

Designed by CREATE | CRT115274A