iNetwork
involve influence inspire

INFORMATION SECURITY
CONFERENCE 2017

Information Security Conference

Thank you for attending iNetwork's third annual Info Sec conference.

In the 12 months, there have been an unprecedented number of high profile cyber attacks that hit the media – from Yahoo!, breach of Democratic National Committee, breach of Bangladesh Bank and the hack of Lincolnshire and Goole NHS.

Information is a key organisational asset and its security is of paramount importance to reduce risk to business processes, reputational damage and loss in consumer confidence. Where this has been compromised, it has resulted in significant issues for the organisations concerned which are increasingly reported in the media.

This conference will help delegates better to respond cyber threats and defend against cyber-attacks.

Getting the most out of your day

Moving around the Venue:
The plenary sessions and exhibition stands will take place on the first floor in the First Floor Hall. 30 minute seminar talks will be held in the first floor hall, seminar room 1 and seminar room 3/4 (on the ground floor). Toilets can be found on both floors.

Car parking:
You will be able to park on Sidney Street but please remember this is restricted to 2 hours on weekdays between 08:00 – 18:00hrs. If you parked at NCP Chester Street (M1 5GE), please remember to validate your parking ticket at Reception (before you leave). This will give you a discount on standard parking charges.

Technology:
FREE WIFI access is available for all delegates and the WIFI Code is: Welcome247.

Twitter:
You are invited to tweet on the day using #infosec2017. iNetwork's Twitter handle is @theinetwork.

QR Codes:
All delegates and exhibitors have been provided with an individual QR code that contains their contact information. This Code will be on all name badge and will allow exhibitors and delegates to share their contact details more quickly. The QR code can be scanned by using a number of devices.

Feedback:
Please don't forget to complete your feedback for each speaker. We like to hear from you.
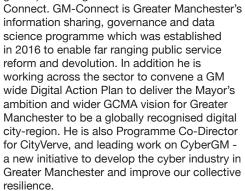
Agenda

Time	Session
08:30 (70 mins)	**Arrivals and networking in Exhibition Showcase area**
09:40 (5 mins)	**Welcome and Opening Address** Phil Swan (Chief Information Officer, GM Combined Authority)
09:45 (5 mins)	**A perspective from the Chair of the North West Warning, Advice and Reporting Point (Video Presentation)** Sarah Gallear (Information Governance Manager, Warrington Borough Council)
09:50 (25 mins)	**Key Note: Current Landscape and Emerging Threats** Lee Carass (Senior Sales Engineer UKI, Trend Micro)
10:15 (20 mins)	**Build your (cyber) house on the rock** Mark Tomlin (Manager – Cyber Security, KPMG)
10:35 (25 mins)	**The real cost of a cyber-attack** Geoff White (Technology Journalist)
11:00 (25 mins)	**National Cyber Security Programme – Building Resilience Together** William Barker (Head of the National Cyber Security Programme Local, Department for Communities and Local Government)
11:25 (30 mins)	**A Plenary Panel Conversation chaired by Phil Swan - Developing an organisational response to the ever-changing threat landscape** Panel Speakers: Helen Williams, Geoff White, William Barker, Lee Carass, Mark Tomlin
11:55 (45 mins)	**Lunch, Networking & Showcase, Delegates move to the seminar rooms**

Time	1st FLOOR HALL	SEMINAR ROOM 1	SEMINAR ROOM 3/4
12:40 (30 mins)	**A Regional response to the current threat landscape** Helen Williams (Cyber Protect Officer, Regional Cyber Crime Unit)	**The future of the IG Toolkit** David Ingham (Senior Project Manager, NHS Digital)	**Co-funding & Collaborating around Cyber Awareness** Jane Hancer (Director of Innovation, CC2i)
13:15 (30 mins)	**Update on Guidance – sharing patient records** Stephen Elgar (Information Governance Specialist – Interoperability, IGA)	**Audits, Data Handling and GDPR** Mark Brett (Visiting Fellow De Montfort University, NLA WARP Programme Director)	**Reflections from the recent WannaCry attack** David Willis (Head of Info Governance WWL NHS Trust)

Time	Session
13:45 (20 mins)	**Comfort Break and Exhibition Showcase**
14:05 (5 mins)	**Welcome Back**
14:10 (20 mins)	**Is your data secure in the cloud?** Prof Conor Ward (Visiting Professor – Queen Mary University of London, Chair Cloud Industry Legal Forum)
14:30 (30 mins)	**A Plenary Panel Conversation chaired by Phil Swan, CIO GMCA** **Striking the Right Balance "Cyber Security versus Digital Opportunity"** Panel Speakers: Professor Conor Ward, Mark Brett, Michael Trevett, Dr Daniel Dresner
15:00 (5 mins)	**Delegates move to the seminar rooms**

Time	1st FLOOR HALL	SEMINAR ROOM 1	SEMINAR ROOM 3/4
15:05 (30 mins)	**Designing a future PSN compliance model** Nick Woodcroft (Designing a future PSN compliance model)	**Implementing effective identity management – VERIFY** Peter Chamberlaim (Technical Architect, GDS)	**Building Skills and Raising Awareness** Dr Daniel Dresner (Academic Coordinator for Cyber Security University of Manchester)
15:40 (30 mins)	**Engaging and Empowering Leadership with the Cyber Security agenda** Michael Trevett (Deputy Director Security, NHS Digital)	**Local Tactical Response to National Cyber Security Strategy** Mark Brett (Visiting Fellow De Montfort University, NLA WARP Prog Director)	**When Hackers attack: The evolving threat landscape** Paul Mason (Training Manager, Ethical Hacker Secarma)

Time	Session
16:10	**Close**

Plenary Speakers

Phil Swan

Phil leads the Digital Service at the Greater Manchester Combined Authority (www.greatermanchester-ca.gov.uk) including GM-Connect. GM-Connect is Greater Manchester's information sharing, governance and data science programme which was established in 2016 to enable far ranging public service reform and devolution. In addition he is working across the sector to convene a GM wide Digital Action Plan to deliver the Mayor's ambition and wider GCMA vision for Greater Manchester to be a globally recognised digital city-region. He is also Programme Co-Director for CityVerve, and leading work on CyberGM - a new initiative to develop the cyber industry in Greater Manchester and improve our collective resilience.

Sarah Gallear

Having been working in the public sector for over 16 years, I have over 8 years' experience in information security and have been specialising in information governance for the past two years. I've been chairing the North West WARP since 2014 and have been a member of the iNetwork WARP since its early days. My interests are technology, cyber security, data protection, breach management and keeping information safe

Lee Carass

Lee is Senior Sales Engineer at Trend Micro and is responsible for advising Trend Micro's UK customers on security transformation and consolidation. Lee has 20 years of experience and has held IT infrastructure and security roles across Yorkshire Post Newspapers, Johnston Press, Civica and before Trend Micro he held the position of Senior Sales Engineer at Sophos. Lee works with customers to understand their risks and develop security strategies that enable business objectives, with focus on digital transformation and cloud.

William Barker

William is a career Civil Servant with over twenty five years' experience of working at the heart of Whitehall and local government on public service reform and digital government agendas.

In his current role he focuses on the interplay between Cyber Resilience, Digital by Default and open policy making, and how they impact on central/ local government and wider public service provision. Previous posts have included senior secondments into local government and working in the fields of e-democracy, constitutional and Civil Service reform.

He is regularly consulted as a contributory author/public speaker on digital innovation by organisations such as LGA, SOLACE, SOCITM, and St George's House. He is at Visiting Fellow at Brunel University.

Geoff White

An award-winning television news journalist, Geoff White's exclusives have covered everything from fraud in the internet dating industry to the shadowy world of Russian cybercrime gangs.

He works mainly for the BBC and Channel 4 News, with a focus on tech security, personal data, privacy and e-crime. He is also the co-creator of The Secret Life of Your Mobile Phone, a live, interactive phone hacking stage performance which shows how the global technology industry is harvesting the data leaking from your handset.

Prof Conor Ward

Conor Ward is a former partner in the international law firm Hogan Lovells, where he was group manager of its London based IP and Technology group specialising in computers and communications law. He is a Visiting Professor at Queen Mary, University of London's Centre for Commercial Law Studies where he teaches the post graduate IT Law course. Conor has extensive experience of advising clients in relation to outsourcing and cloud services as well as advising in relation to, and following, cyber security incidents including in dealing with the aftermath of such incidents such as liaising with regulators, advising in relation to legal actions against the perpetuators and helping clients deal with law enforcement and criminal prosecutors.

Conor is also a board member of the Cloud Industry Forum (CIF) and chairs the Cloud Industry Legal Forum which advises on Cloud Computing Legal Issues.
NHS Digital to help implement the new Data Security Standards for Health and Care published in Dame Fiona Caldicott's review in June 2016.

Helen Williams
A Regional response to the current threat landscape

Helen Williams has worked for Merseyside Police for 10 years. She joined the North West Regional Organised Crime Unit (Titan) in May 2014 as Cyber Protect Officer. She works alongside officers in the regional cyber-crime unit who investigate malware, network intrusion and denial of service attacks.

Her role is part of a national network linked to the UK Government's National Cyber Security Centre and aims to help businesses and the community, by providing information about cyber threats, advice on how to protect data and online assets and, free resources to help individuals stay safe online.

Michael Trevett
Engaging and Empowering Leadership with the cyber security agenda

A graduate of Information Systems, Mike's database and systems experience began with BT in the early 1990's. Since then he has worked in the telecommunications, retail, automotive and financial services sectors, latterly as a CISO, before joining the Civil Service at the Office for National Statistics (ONS) in 2009. Whilst at ONS, Mike took on responsibility for the full protective security and assurance portfolios before joining Cabinet Office as the Head of the Office of the Government Senior Information Risk Owner. In late 2016, Mike joined NHS Digital to help implement the new Data Security Standards for Health and Care published in Dame Fiona Caldicott's review in June 2016.

Jane Hancer
Co-Funding and Collaborating around Cyber Awareness

Working across digital government for the last 15 years - in fact a little longer if you count the time spent in the early dotcom days spearheading public access to government data - we set up CC2i: Co-fund & Collaborate to Innovate in summer 2016. Bringing the proven crowdfunding model into a public sector setting, I am charged with driving campaigns, working with partners, finding innovation and collaboration opportunities - from both within the public sector and SMEs - to deliver digital solutions that better fit public sector needs and make best use of budgets.

Stephen Elgar
Update on Guidance – sharing patient records

Stephen Elgar is a specialist in confidentiality and security for sharing patient records. He supported the roll out of these record systems in London for many years and has been part of the NHS Digital team for the last 4 years. He took a degree in Geography, trained as a Nurse, has an MSC in Information Security and is a CISSP member.

Mark Brett
Audits, Data Handling and GDPR, Local Tactical Response to National Cyber Security Strategy

Mark has 30 years experience in Local, Regional and National Government roles. A former CIO and Chartered Manager, Mark recently spent three years working with the PSN Programme as Lead IA Advisor and PSN SOC/Security Manager. He continues to lead the Local Government IA work through the NLAWARP and as a special advisor to the Local CIO Council and Socitm. Mark is an honorary Visiting Fellow (Cyber Security) at De Montfort University, lecturing on the Cyber Security MSc and is reading a PhD in Cyber Security

Nick Woodcraft
Designing a future PSN compliance model

Nick is Senior Technical Advisor at Government Digital Services and prior to that was Applications Product Manager, Common Technology Services at Government Digital Services.

Peter Chamberlin
Implementing effective identity management

Peter Chamberlin is a technical architect working on GOV.UK Verify, and has been focussed on architecture for identity since joining GDS Government as a Platform in 2016. He has extensive experience in building web technologies at scale, and prior to joining the Civil Service worked as a principal developer at BBC News.

Dr Daniel Dresner
Building Skills and Raising Awareness

After 22 years with NCC, Daniel founded The Dresner Associates to detect human vulnerabilities in networks, and mend the often broken threads that bind information together. Over 1000 students have studied cyber security and governance with him at The University of Manchester and engage in his research projects.. His key works include the Green Surf Code for Children, Desert Island Controls for Business, and The Three Universal Laws for Information and Cyber Security (with Neira Jones).

David Ingham
The future of the IG Toolkit

David Ingham is Senior Project manager on the Re-Designed the IG Toolkit project.This is large scale across health and care project with significant stakeholder engagement across a range of health, care and ALBs. David is an experienced project manager who has worked across local authority and health.

Paul Mason
When Hackers attack: The evolving threat landscape

Paul Mason is the Training Manager for cybersecurity firm Secarma. He is an ethical hacker, a deeply experienced educator and finalist in a number of international cybersecurity challenges. His advice is regularly sought by government departments including Police Scotland, educational bodies and commercial clients requiring security testing. Fusing his joint passion for technology and teaching, Paul has worked as a security consultant and more recently developed cybersecurity qualifications for the Scottish Qualifications Authority and the Department of Education alongside bespoke staff security training for companies and organisations. Paul likes monkeys.

David Willis
Reflections from the recent WannaCry attack

David is Head of Information Governance at Wrightington, Wigan and Leigh NHS Trust. He has MSc Forensic Computing and is a CISSP Certified Information Security Professional with over 25 years experience.

Reflections from the recent cyber-attacks - Petya - Not Petya and WannaCry are that timely communications is key to be able to respond quickly to threats and attacks. This was particularly noticeable during the Wanna Cry attack as organisations that participate in the North West Warning, Advice and Reporting Point (North West WARP) received early notification of the ransomware attack which enabled organisations to take timely and necessary action.

The North West WARP is a service available to all iNetwork member organisations. It provides a trusted community for information security professionals and a forum for colleagues to learn from peers and experts within and outside the Group. Members are able to confidently receive and share up-to-date advice on information security threats, incidents and solutions. It is designed to facilitate appropriate vigilance in a timely and cost effective way.

Hear what one of the WARP members has to say about North West WARP...

Please could you tell us who you are, job role and organisation?

"I'm Debbie McCarron and I'm a Senior ICT Consultant at Salford City Council. I started at the council 11 years ago as an IT Trainer and moved into my current role in 2009.

My role includes the non-technical aspects of information security; user awareness, policy writing, compliance (PSN, PCI, ISO 27001, IG Toolkit), ad hoc advice for Data Sharing/Data Processor's Agreements, tenders, contracts where info sec is relevant, etc.

I'm also tasked with continual service improvement, the main area being the way in which our customers interact with us, raise work requests etc. A fair bit of my time is taken up with network accounts; giving advice and approving/rejecting ad hoc requests for access."

What are the key benefits to you and your organisation from being a member of the North West WARP?

"The ever-changing landscape of security and compliance can be a real challenge; so being part of a group that you can call upon, and rely on, to help and keep you informed is a great asset.

I think the biggest benefit is the collective voice; a single council complaining to a central government department about a particular aspect of their standard would fall on deaf ears, whereas the WARP is heard. Getting PSN assessors to attend events so we actually got to speak to them face-to-face was a real benefit for me.

The WARP is a great go-between; I had a dilemma where I had a question for the Cabinet Office but I didn't want to divulge how we were currently doing something that could affect our PSN Coco. But Ajike kindly asked the question on my behalf, keeping my identity anonymous.

Another true benefit is hearing about upcoming changes and having chance to give input/feedback."

What would you say to colleagues who are curious about joining the North West WARP?

"The ever-changing landscape of security and compliance can be a real challenge; so being part of a group that you can call upon, and rely on, to help and keep you informed is a great asset.

I think the biggest benefit is the collective voice; a single council complaining to a central government department about a particular aspect of their standard would fall on deaf ears, whereas the WARP is heard. Getting PSN assessors to attend events so we actually got to speak to them face-to-face was a real benefit for me.

The WARP is a great go-between; I had a dilemma where I had a question for the Cabinet Office but I didn't want to divulge how we were currently doing something that could affect our PSN Coco. But Ajike kindly asked the question on my behalf, keeping my identity anonymous.

Another true benefit is hearing about upcoming changes and having chance to give input/feedback."

If you would like to find out more information about the WARP and benefits for your organisation, you can email the Co-ordinator, Ajike Alli-Ameh at ajike.alli-ameh@tameside.gov.uk – or catch her for a quick word at the conference today!

TrendMicro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints.

All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection.Optimized for leading environments, including Amazon Web Services, Microsoft®, VMware®, and more, our solutions enable organizations to automate the protection of valuable information from today's threats.

Trend Micro customers include 45 of the top 50 Fortune® Global 500 companies, and 100% of the top 10 global automotive, banking, telecommunications, and petroleum companies.With over 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud.

Egress

Egress Software Technologies is the leading provider of data security services designed to protect shared information throughout its lifecycle.

Offering customers in the Public and Private Sectors a portfolio of complementary services, the Egress Switch platform enables end-users to share and collaborate securely, while reducing the risk of loss and maintaining compliance. These award-winning integrated services include email and document classification, email and file encryption, secure managed file transfer, secure online collaboration and secure archive.

Certified by Government, Switch offers a seamless user experience, powerful real-time auditing and patented information rights management, all accessible using a single global identity.

IGA

The Information Governance Alliance (IGA) mission is to enhance the quality of health and care services, including people's experience of using those services, by improving information governance. We aim to improve information governance in health and care by:
• being an authoritative source of advice and guidance
• providing support to organisations to help them and their staff handle personal information confidently and in the best interests of people who use their services
• developing the leadership and culture of health and care services to promote legal and secure information sharing, and
• developing the capacity and capability of information governance professionals, by providing expert advice and supporting knowledge sharing networks.

Data Protection People

Based in Leeds, Data Protection People has customers all over the UK and a handful in Europe. Our team of data protection experts have first rate experience in senior roles in the public and private sector in the field of information governance and data protection management as well as with the regulator, the Information Commissioner's Office.

Their academic underpinning is of the highest quality boasting post-graduate and professional qualifications in the field of information rights law and data protection practice. For more information visit: http://www.dataprotectionpeople.com/

THE RANSOMWARE X.
THE CLICK-HAPPY X.
THE COSTLY X.

Solve it with XGen™ cyber security.

WHAT'S YOUR X?

Go beyond Next-Gen
with XGen™ cyber security.

trendmicro.co.uk/xgen