CRESTCon – Stream 1

Wolfson Theatre

Stream hosts: **Paul Midian and Mark Turner**

09:40 – 10:25

Keynote: The changing face of security – a view from the 'C' suite

Chris Ulliot, CISO, RBS

Someone once said that "What got you here, won't get you there" and as CISO for a large financial institution, Chris believes it's becoming increasingly clear that the security industry needs to evolve. As someone who has moved from the consultant side of security to the consumer of the security industry, Chris will talk on how the security industry doesn't always help the customer and on occasions, how the best intentions can have unintended consequences. Sharing what a bank looks for from the technology and services it consumes, this presentation will aim to look at how the security industry can better partner with organisations to achieve the goal of providing a more secure environment for all.

Chris has a career that spans over 25 years in technology and has held a number of roles in both the public and private sectors. With experience ranging from micro electronics through to international telecoms systems and large, online transactional systems, his experience has resulted in him advising on how to secure some of the countries most critical assets. For the last 12 years Chris was a Technical Director at CESG (now part of the National Cyber Security Centre) and in January 2016 moved to RBS as the bank's CISO.

10:30 – 11:00

Incident remediation: lessons learned on the front lines

Jeff Hamm, Technical Director
Manfred Erjak, Principal Consultant, Mandiant Security

Recovering from a large-scale incident is not an easy task. When compromised by an Advanced Persistent Threat, one must plan the efforts ahead of time to succeed in fully remediating and eradicating the attacker from the environment. This presentation combines elements of a holistic investigation covering up to tens-of-thousands of machines. It includes specific knowledge on how to best remediate from such an event. The presenters will talk about the different stages of preparation, when it is the best time to remediate and how to classify actions. This is also in pursuit of the organisation becoming an "Investigation Ready" Environment. They will also include examples of real investigations and remediation efforts to illustrate common complications like remediating too early, remediating partially and working with third-party IT providers.

Jeff Hamm has been employed with Mandiant since 2010 and is a Technical Director assigned to the Europe region, where he manages a team that conducts forensic examinations and incident response. Response and examinations range from a single host to over 100,000 hosts on a network. He has also worked part-time as an adjunct lecturer at NTNU (Norwegian Science and Technology University) in Gjøvik, Norway since 2011. There he provides intense practical labs based on real world computer forensic incidents using both Windows

and Linux servers and attack systems. He has co-authored “Digital Forensics” edited by Andre Arnes in 2017 for academia and practitioners.

Manfred Erjak has been employed with Mandiant since 2015 and is currently a Principal Consultant. He is a trusted Information Security advisor and expert IT Network Engineer consultant to global corporations with 20 years of experience in secure network design and architecture, strategic corporate security system and governance development, and incident response investigations. Manfred creates innovative and effective solutions to the most challenging and sensitive cybersecurity situations with exceptional analytic abilities. He has significant experience working with utilities, manufacturing, technology, pharmaceutical and Fortune 500 companies.

11:30 – 12:15

Common traps and pitfalls in red-teaming

Andrew Davies, Director
Jon Medvenics, Lead Incident Manager, Netscylla

This presentation provides an overview of some of the common techniques in today’s red-teaming, contrasted against blue-team methodology and vendor solutions. A humorous take on how to catch a red-teamer; featuring log analysis, implant and payload reversing and fingerprinting, and OSINT against suspected red-teamers. It will also highlight the tools and techniques used by blue-teamers that can help red-teamers improve their game.

Andrew Davies is an experienced red-teamer and penetration tester who has performed two CBEST engagements and several global red-team assessments across multiple sectors in the last three years. Having recently been deployed in an organisation within a ‘purple team’, he has used his experience to aid in fighting off real world attackers and other red teamers. Andrew has discovered new tools and techniques that could be beneficial to other offensive security testers in the industry.

Jon Medvenics is a blue-teamer and Lead Incident Manager who currently leads the response team for a public sector organisation primarily focused on network monitoring, malware analysis and threat hunting, to rapidly respond in a crisis. Jon has put his experience to the test through blue team assessments and NATO sanctioned war-games and has found immeasurable benefit from working closely with the reds to improve his skills. As a big advocate for closer collaboration, he’s keen to share his experiences and thoughts.

12:20 – 12:50

I know what you installed last summer

Saurabh Harit, Managing Security Consultant Spirent

If you search through Exploit-db, there are over 10,000 remotely exploitable vulnerabilities that exist in numerous 3rd party web applications and could allow an attacker to completely compromise the back-end server. These vulnerabilities range from remote code execution to malicious file uploads to SQL injection.

With all the modern network protections these days, a dedicated attacker is always looking for just weakness to penetrate through the network. Most of these applications are installed as part of the test and trial process and are often configured weakly. In this talk, Saurabh will elaborate on how such applications could lead to the compromise of the complete infrastructure. He will also introduce an open-source tool that could be used to detect such applications on the network.

Finally, Saurabh will talk about some of the best practices that developers and IT teams could adhere to, in order to securely configure such 3rd party applications.

Saurabh Harit is an experienced security consultant who has delivered countless penetration testing and security consulting services to organisations across the globe. He has worked at reputed security consulting firms such as Trustwave, Security Compass, SensePost and Honeywell. During his industry experience of over 12 years, Saurabh has worked across diversified industry verticals such as Banking, Aerospace, building solutions, Process & Control Systems and has developed expertise in various aspects of Information security.

Saurabh specializes in web application and network security, with a secret crush on binary reverse engineering. He has contributed towards proof-of-concept exploits and white papers in the infosec domain as well as delivered security training to various fortune 500 clients globally and at reputed security conferences such as CansecWest and Black Hat. Saurabh has presented his research at several security conferences including Derbycon, Toorcon, BSides Toronto, Hack3rcon & BlackHat Europe.

13:50 – 14:15

Hacking an ISP's home router from the web

Daniel Cater, Lead Security Consultant, Context Information Security

This talk will demonstrate how a remote attacker can compromise an ISP-provided router using web-based methods only - no screwdrivers or soldering irons required. Multiple vulnerabilities are chained together to compromise the router, leading to subsequent attacks - such as being able to connect to the customer's Wi-Fi, hijack their DNS results, or read their sensitive files from an attached USB memory stick.

Daniel Cater is a Lead Security Consultant at Context Information Security. Previously a software developer for an investment bank, he now prefers trying to break things rather than make things. He holds the CREST Certified Tester for Web Applications certificate (CCT App) and enjoys hunting for bugs in web applications and web browsers, as well as doing research into big data, cloud security and consumer products.

14:20 – 14:45

Nematodes and neotodes

Matt Wixey, PwC Vulnerability, Research Lead

Worms are probably the most destructive and indiscriminate form of malware. For many years, the prospect of network worms exploiting unpatched vulnerabilities in systems and automatically spreading throughout the internet struck fear into the hearts of many sysadmins and network defenders. However, after the introduction of security mechanisms such as DEP and ASLR, the risk of traditional network worms dropped sharply. Nowadays, would-be worm authors tend to rely either on other infection vectors, such as removable storage media, or web application vulnerabilities, and incidents like WannaCry have become the exception rather than the norm. This presentation will cover two unusual and seldom-discussed aspects of worms. First, the concept of nematodes or anti-worms, which exploit the same vulnerabilities as malicious worms but then automatically patch security flaws. Second, it will cover the concept of neotodes - a term the presenter has coined to describe a new breed of worms which don't rely on traditional infection vectors to spread. Examples include worms which attack and spread using Wi-Fi, RFID, light, sound, and more.

Matt leads vulnerability research for PwC's Cyber Security practice in the UK and works on the UK Ethical Hacking team. Prior to joining PwC, he worked for the Metropolitan Police Service, leading a technical R&D team within a Specialist Operations unit. His research interests include antivirus technologies, exploit development and RF security.

14:50 – 15:20

Danger of client side controls - E2E encryption

Anton Bolshakov, Managing Consultant, ITDefence Singapore

The security level of mobile / web applications increases. Pentesters face multiple challenges before they can intercept traffic and start testing their target. Jailbreak detection, certificate pinning (hardcoded or HPKP), MDM solutions (traffic tunnelling), non-standard parameter formatting and client side encryption are just a few examples of such client controls. Many organisations fully rely on such controls and challenge pentesters to demonstrate their effectiveness. Using End-To-End (E2E) encryption as an example, this presentation will show that client-side solutions are largely ineffective and in some cases can even expose an organisation to unexpected risks. The presentation will show real case examples starting with a simple AES javascript encryption and conclude with more complex two-side encryptions wrapped in various encodings. Anton will also release a burpsuite plugin that helps to bypass such barriers and allows the discovery of vulnerabilities, which could be hidden for many years despite multiple rounds of penetration testing.

Anton is a Managing Consultant with ITDefence based in Singapore. He is a highly experienced security consultant having previously held the role of Manager in the Performance and Technology Practice and member of the Information Protection and Business Resilience Team at KPMG LLP and Senior Security Consultant at Dimension Data. Anton has managed and executed hundreds of security assessment projects across Government, Telecommunications and Financial Services sectors in the APAC Region. He is held in high regard by clients and his peers for his knowledge and skills in vulnerability identification and exploitation.

Breakout session

15:20 – 15:50

Ask the Assessors:

Steve Bates, Oliver Church, Ian Lovering & Stuart Morgan. Chaired by Stuart Criddle

A specially assembled panel of experienced assessors will be answering questions on CREST examinations.

16:00 – 16:45

CSRF is dead, long live CSRF!

Daniel Tomescu, Associate Manager, KPMG Romania

Recently removed from OWASP Top 10, Cross Site Request Forgery (CSRF) vulnerabilities used to rule the world of web applications. Impressive in simplicity and effectiveness, CSRF was the plague that threatened to extinct multi-tab browsing. However, after years of "vaccination" with CSRF Tokens and other medication, CSRF is dead. A plague of the past. Right? Well, not really. A few mutations, some unimmunised hosts and a bit of imagination can result in the rebirth of CSRF into a deadly, 'beautiful' vulnerability. The presentation will cover common scenarios which can allow an attacker to: pivot from the internet to your internal network; jump from one browser to another; uncover your secret internet identities or unveil your darkest secrets. All the above scenarios, may sound apocalyptic and science-fictional, but can be reproduced because Cross-Site Requests are still fair game. Long live CSRF!

A Security Consultant in the Penetration Testing Team at KPMG in Romania, Daniel is passionate about web security, mobile and embedded devices. He likes to challenge himself by participating in bug bounty programs and the results are that several companies (including Red Hat, Mozilla and Twitter) recognised his efforts by adding him in their Hall of Fame pages. His latest work includes PhotoBear – software that allows hiding information in images - and his license thesis – "Securing the access to a premises using Bodycom technology".

16:45 – 17:30

The big debate: CISOs from CREST Industry panel and Senior Pen Testers

Chaired by Nicola Whiting, COO, Titania

Nicola Whiting is an experienced Chief Operations and Strategy Officer with a strong history of working in Cyber Security / InfoSec. She Specialises in enterprise security automation software (self-healing networks), business development, trust-based selling and neuromarketing.

An advocate for Autism and Women in Cyber, she provides government level advice on Diversity and is Worcestershire's Commissioner for the UK Cyber Science & Innovation Audit.

She is an engaging public speaker and writes for publications such as The Huffington Post, Defence Contracts Bulletin, Defence News Online and Signal. Keynote topics include "The Rise of Automated Attacks", "The Future of Automated Cyber Defences" and "Hacking the Human Brain".

In 2017 Nicola was named by SC Magazine as one of the Top 20 most influential women working in cyber security.

The CREST Industry Panel

Paul Midian, Chief Information Security Officer, Dixons Carphone PLC

Paul is an accomplished information and cyber security practitioner with over 20 years' experience; he is Chief Information Security Officer at Dixons Carphone plc. Previously, Paul was a director in the Cyber Security practice at PwC leading large scale information and cyber security improvement and transformation programmes. Prior to his role at PwC, Paul was a director at Information Risk Management Plc . During his tenure revenue increased by over 75% and the company won the Secure Computing 'Information Security Consultancy of the Year 2013 award. Prior to working at IRM he was Head of Security Testing at Siemens Enterprise Communications (formerly Insight Consulting). Paul is a member of the BCS and of ISACA. He has been involved in the CREST organisation since its inception.

Nick Bleech, Head of Information Security Travis Perkins

Nick Bleech has led Information Security at Travis Perkins since 2013, and has worked in this field since 1986. He started in security engineering R&D, then onto consulting, ITSEC evaluation, pentesting, and audit in several Financial Services, Oil & Gas, Aerospace and Consumer Markets firms, as well as the Public Sector; and progressing to security management roles. He was a founding board member of The Jericho Forum in 2004, early advocates of what is now known as Cloud Security. He was IT Security Director at Rolls-Royce from 2004-8, where his team tackled early APT attacks on the UK high-tech sector and he led cross sector collaboration in response, as industry chair of the CPNI Aerospace & Defence Manufacturers' Information Exchange.

The Senior Pen Testers

Stuart Criddle, Principal Consultant, NCC Group

Stuart is one of the two Assessors' representatives on the CREST Executive and leads on the technical delivery aspects of CREST examinations. Stuart is an Executive Principal at NCC Group responsible for leading large complex projects and managing testing teams on both infrastructure and application assignments and has a long history of working with central government, MOD and police clients. With previous experience in both CLAS and QSA role, Stuart has a wide experience of risk management and dealing with senior customer representatives to explain technical issues in language that senior management understands. Stuart has an interest in IoT, RF, hardware and automotive technologies and continues to work to build capabilities in these areas.

Ken Munro, Partner, Pen Test Partners

Ken is a regular speaker at the ISSA Dragon's Den, (ISC)2 Chapter events and CREST events, where he sits on the board. He's also an Executive Member of the Internet of Things Security Forum and spoke out on IoT security design flaws at the forum's inaugural event. He's also not averse to getting deeply techie either, regularly participating in hacking challenges and demos at Black Hat, 44CON, DEF CON and BSides amongst others.

Ken and his team at Pen Test Partners have hacked everything from keyless cars and a range of IoT devices, from wearable tech to children's toys and smart home control systems. This has gained him notoriety among the national press, leading to regular appearances on BBC TV and BBC News online as well as the broadsheet press. He's also a regular contributor to industry magazines, penning articles for the legal, security, insurance, oil and gas, and manufacturing press.

IISP Congress – Stream 2

Seligman Theatre

Stream host: **Jill Trebilcock**

09:40 - 10:25

Keynote: Alternative Routes, or how to beat the skills gap

Thom Langford, CISO, Publicis Groupe

Increasing cybersecurity threats mean most organisations are looking to grow their cyber and Information Security teams. However, this also means that the existing shortage in qualified, experienced security people is getting worse.

In this session Thom will share the approach he has taken to tackle the Security Skills shortage by looking for "passionate people and inspire them" rather than trying to find CVs that tick the appropriate boxes. He will challenge us to look beyond just qualifications and experience and think about the potential of candidates from non-traditional Security backgrounds giving opportunities that benefit both them and the business.

As Chief Information Security Officer of Publicis Groupe, Thom is responsible for all aspects of information security risk and compliance as well as managing the Groupe Information Security Programme. Additionally, in the role he is responsible for business continuity capabilities across the Groupe's global operations. Having successfully built security and IT programmes from the ground up Thom brings an often opinionated and forward-thinking view of security risk, both in assessments and management, but is able to do so with humour and pragmatism. An international public speaker and award-winning security blogger, Thom contributes to a number of industry blogs and publications. Thom is also the sole founder of Host Unknown, a loose collective of three infosec luminaries combined to make security education and infotainment films.

10:30 - 11:00

Why cloud security is different

Paul Schwarzenberger, Cloud Security Architect & DevSecOps, Financial Services, and Associate Trainer, QA

One misconfigured line of code results in anyone in the world being able to destroy or take over a production system in the cloud…

Paul presents examples and demonstrations of real life cloud security issues based on his experience working on cloud migration projects and operational cloud applications for both public and private sector organisations. He then discusses the root causes of these issues, and how best to mitigate cloud security risks, looking not only at technical controls such as automated testing and compliance enforcement, but also aspects such as knowledge, training, culture and organisational structure.

Paul is a Cloud Security Architect and DevSecOps specialist with 15 years' experience leading a wide range of security related engagements for customers across sectors including financial services, pharmaceutical, retail, education and media, logistics, UK Government and Police. He uses an agile DevSecOps approach to lead the implementation and migration of critical systems to public cloud, with demanding security and compliance requirements for protection of personal data, detection and prevention of cyber-attacks and financial fraud. The training course Paul recently developed for QA, Practitioner Certificate in Cloud Security, was the first ever cloud security course to be awarded GCHQ Certified status.

Paul has numerous security qualifications, certifications and memberships including MSc Information Security Royal Holloway with distinction, M.Inst.ISP, CCSP, CISSP and AWS Certified Solutions Architect - Associate.

11:30 – 12.15

If only it were just the GDPR!

Stephen Bonner, Partner, Deloitte,
Nick Seaver, Partner, Deloitte

If only it were just the GDPR. Then life would be…easier? Perhaps, but that's not the world of 2018. In addition to the GDPR, organisations across all industries have to make sense of an international tangle of cyber security regulations, frameworks, guidelines, recommendations, and regulator 'suggestions'. Security professionals have to untangle this Gordian knot while receiving scrutiny from business leaders (on the inside) and threat actors (inside and outside). So what's an overworked CISO supposed to do?

In this session, Stephen Bonner and Nick Seaver will look at cyber security regulatory trends and offer examples from their experience in financial services, which is very often at the forefront of regulation development. They will identify areas where efficiencies can be made now, where long-term thinking is the priority, and where (if anywhere) you can sit back and relax. Only one thing is certain, the regulatory landscape is becoming more complex, get one step ahead by attending this session.

Stephen is a Cyber Security Partner focused on Financial Services. Before his five years of Big4 consulting experience, he was Group Head of Information Risk at Barclays. He was inducted into the InfoSec 'Hall of Fame' in 2010 and was number one on the SC Magazine/ISC2 'Most Influential 2010' list.

Nick is a Partner within Deloitte, responsible for leading on UK and EMEA Cyber Risk services within the financial services industry and has significant experience of both cyber security and technology risk/audit within financial services. In addition to his client focus, Nick has significant internal responsibilities for cyber recruitment, team development and marketing. Nick is both a Member of the Institute of Information Security Professionals (IISP), and a board member, holding the position of treasurer. He is also a qualified accountant (FCCA), and has an Executive MBA with a dissertation on "Information Leakage in UK Financial Services". He is quoted frequently in the press and regularly speaks at conferences on cyber related topics.

12:20 – 12:50

Building a Security Conscious Culture

Melanie Oldham, Founder, Bob's Business

Explore the steps to creating a security conscious workforce. By understanding the way users behave and learn, attendees can learn how to create and execute awareness and training campaigns that their users will truly buy into. When performed correctly, awareness campaigns have the power to be more than just a tick box exercise, causing a true culture change that can be permanently embedded within the backbone of an organisation. Creating a training programme that is accessible at every level and addresses every level of ability is paramount in engaging the workforce, and Melanie will demonstrate how this can be achieved with some simple but effective steps that delegates can take away and apply to their working environment. Delegates will discover the actions they can take to create a truly engaging awareness campaign that is accessible at all levels and that can deliver strong results for organisations and its employees.

Melanie Oldham is the founder and driving force behind Bob's Business, an award winning cyber security awareness training and phishing simulations provider. Melanie has racked up over 10 years' experience in the cyber security sector and has become a reputable and well-respected force within the industry.

Bob's Business has delivered awareness campaigns to organisations of all shapes and sizes, from 10 users through to 70,000 users. In 2017, they educated over 500,000 users.

13.50 – 14:15

Things in the fog

Prof Paul Dorey PhD, CISM, F.Inst.ISP

Perhaps the most important lesson an information security professional can learn is not to be caught out by the unexpected, be it a business change, new business relationship or the adoption of a new technology. Cloud computing challenged our thinking to go beyond the corporate network, but that's nothing to the wild ride combination of the Internet of Things both at the edge and combined with the cloud and AI. I am going to look at the security challenge of the next decade and how some are starting to deal with it.

Prof. Paul Dorey, is well known for his strategic thought leadership in cybersecurity including being Founder Chairman of the Institute of Information Security Professionals and now Chairman of the Internet of Things Security Foundation. His award winning career in Cybersecurity Risk Management includes Executive leadership roles at Deutsche Bank/Morgan Grenfell, Barclays Bank and BP.

Now a Visiting Professor in information Security at Royal Holloway, University of London, he works with companies and government departments in developing their long term cybersecurity strategies, their security capabilities and leadership. He recently contributed to the January 2017 World Economic Forum guidance 'Advancing Cyber Resilience: Principles and Tools for Boards' and co-authored 'The Weakest Link' a management guide to security behaviours, awareness and cultural change, published by Bloomsbury. He also acts as an expert witness in cybersecurity cases.

14:20 – 14:45

IoT devices - not a product, more a risk in a box

David Alexander MSc F.Inst.ISP. FBCS, Managing Consultant, PA Consulting

David will be talking about the security of IoT devices; They're not a product, They're a risk in a box. While there are organisations working to develop secure IoT products and architectures, there are far too many products already deployed that are very easy to compromise because of poor design. In the race to the bottom for the time taken to get a new product to market and the drive to minimise the unit cost, the first casualty of any design process is often the security of the design. David will be discussing what can be done to manage those risks.

David is Head of IoT security capability for PA Consulting. He has 28 years of experience in information security, including smart metering, smart grids, Industrial Control Systems and the Internet of Things. He was Head of Security Architecture for the UK smart metering program, leading the work to design the end-to-end security architecture and PKI cryptography for the UK infrastructure, working on the protocols and cryptography for the smart meters, communications hubs. David is a Fellow of the IISP and the BCS. He has an MSc in Information Security from Royal Holloway, is a Chartered SABSA Security Architect and co-author of the textbook "Information Security Management Principles".

14:50 – 15:20

Security interoperability and automation

Nick Humphrey, CTO, Huntsman

Increasingly large and complex mixtures of security point solutions, coupled with a lack of security-skilled operators to drive and interpret the outputs from them, presents a challenge to organisations. Interoperability between competing vendors still leaves much to be desired, and automation can invite distrust and fear of change. In this talk we look at interoperability efforts such as OpenC2, the impact of impenetrable magical boxes being labelled as artificial intelligence, and the importance of context from the human element of security.

Nick Humphrey is responsible for developing and delivering the strategic technology plan, and guiding R&D into security intelligence capabilities to align with new requirements emerging from the customers and industries the company serves.

Nick has over 15 years' experience in cyber security, most of those with UK national security and law enforcement agencies. Prior to joining Huntsman Security, Nick has worked on secure application design and network architectures, security incident investigation, and the creation of threat intelligence programs. He developed a variety of counter-terrorism technologies with the Metropolitan Police Service, was the EMEA Information Security Manager for Marsh & McLennan Companies (MMC Inc.) and before that, served with the UK Ministry of Defence.

Nick graduated with distinction from Royal Holloway (University of London) with a Master's of Science degree in Information Security, and also holds a number of professional technical and security certifications.

16:00 - 16:45

Futurist academic research into AI

Professor Bill Buchanan, Edinburgh Napier University

Bill Buchanan is a Professor in the School of Computing at Edinburgh Napier University, and a Fellow of the BCS and the IET. He was appointed an Officer of the Order of the British Empire (OBE) in the 2017 Birthday Honours for services to cyber security. Currently he leads the Centre for Distributed Computing, Networks, and Security and The Cyber Academy **thecyberacademy.org**. Bill has also published 28 academic books and over 250 academic papers.

His main research focus is around information sharing, such as using Trust and Governance Policies, threat analysis, cryptography, and triage within digital forensics. This has led to several World-wide patents, and in three highly successful spin-out companies: Zonefox **zonefox.com**; Symphonic Software **www.symphonicsoft.com**; and Cyan Forensics **cyanforensics.com**.

Bill regularly appears on TV and radio related to computer security, and has given evidence to both the UK and Scottish Parliament. He has been named as one of the Top 100 people for Technology in Scotland for every year since 2012, and was also included in the FutureScot "Top 50 Scottish Tech People Who Are Changing The World". Recently his work on Secret Shares received "Innovation of the Year" at the Scottish Knowledge Exchange Awards, for a research project which involves splitting data into secret shares, which can then be distributed across a public Cloud-based infrastructure. He was also included in the JISC Top 50 Higher Education Social Media Influencers, and has an extensive online presence, including with asecuritysite.com.

16:45 – 17:30

Disruptive Cyber Security

Sharon Barber, Chief Security Officer, Lloyds Banking Group

As we continue to witness cyber attacks on an unprecedented scale, we must adapt our counter approaches. From ransomware attacks that devastate local communities, to record-breaking DDoS attacks and cyber heist that impact businesses and consumers, this challenging threat landscape spotlights the need for rapid change in organisations' approaches to cyber security. In this session, Sharon Barber, Chief Security Officer, Lloyds Banking Group, outlines pre-emptive, proactive approaches to cyber security and the importance of collaborative working across public and private sectors in this field. Sharon will explore the ways that attacks might be anticipated and discusses how these insights can be incorporated into organisations' "people, process and technology" response. Join the discussion with Sharon on innovative strategies, embracing emerging technologies and public/private partnerships to disrupt the status quo.

Sharon was appointed the Lloyds Banking Group Chief Security Officer in September 2017, bringing together security governance, assurance, monitoring and incident management into a single function with Group wide accountabilities.

Her main focus for security is to continue laying the right foundations to keep pace with the constantly evolving threat landscape and ensuring security has the best people capability, processes and

technology to effectively manage security risk, enabling sustainable growth of our increasingly digital businesses.

Sharon joined Lloyds Bank in 1985 and has held roles including IT Security Director, IT Cyber Security & Risk Director and IT Cyber Security & Major Risk Programmes Director which, alongside her IT Cyber Security responsibilities, saw her managing major IT risk reduction programmes covering Cyber, Technology Currency and IT Resilience.

BCS Security Conference – Stream 3

Council Chamber

Stream hosts: **Adam Thilthorpe**

09:40 – 10:25

What all IT professionals should know about cyber security

Andy Taylor, Aquila Business Services Ltd, BCS Examiner/ Author, APMG Assessor.

Cyber security is not an IT problem – it is a business problem. So, how can IT security professionals address this within the business/ organisation if they are to achieve their security aims? IT technical solutions are only one part of the answer and cannot address all aspects – Andy will address what is required of IT professionals to establish good business processes, to design security in from the start, and to ensure agility in security and service management to protect against whatever threats and attacks the criminals will throw at everyone.

Andy Taylor has been involved with information assurance for over 20 years, starting when he served in the Royal Navy as a security officer. After leaving the Royal Navy, he chose a further career in consultancy and has provided information assurance advice to a wide variety of organisations in both the public and private sectors including the Health Service, Home Office, utility regulators, the Prison and Probation Services and web developers. Andy has a passionate interest in maintaining the highest standards of information assurance and helping others to gain expertise in it.

Andy is a Chartered IT Professional and Fellow of the British Computer Society, a Fellow of the Association for Project Management and an Associate Member of the Institute of Information Security Professionals. He is also a Certified Management Consultant with the Institute of Consultancy and a registered PRINCE2®, MSP™ and Project and Programme Management Consultant with the APMG.

10:30 – 11:00

Giving people the best chance, to be your best line of defence

Bruce Hallas, Managing Director, Marmalade Box Ltd, BCS Author

A strategy to influence 'the human factor' must be based on an understanding of what makes us human and not machines. Raising awareness, influencing behaviour and embedding values into every day culture is not a challenge unique to the cyber security industry. Bruce will draw on his research, into re-thinking the human factor, to identify some fundamental challenges to current approaches to security education, awareness and culture, and how we might learn to address these differently by drawing on experiences from within health, finance and others areas of day-to-day life.

Bruce Hallas is Managing Director at Marmalade Box Ltd, and has worked for over 18 years as an information security manager, practice manager and consultant to lead or support positive change within organisations towards managing risks associated with information and information systems. This support has been delivered through governance, risk and compliance programmes of work and the development and execution of security awareness, behaviour and culture strategies utilising his own methodology called SABC™. Bruce is as an advocate of the role of the human factor in information security, which he promotes through speaking engagements, a podcast on "Re-thinking the Human Factor", blogging, industry publications and a soon-to-be-published BCS book: Cyber Security ABCs.

11:30 – 12:15

Launching CREST Apprenticeships - securing in-demand cyber skills through work-based learning

Jeremy Green, IT Instructor, Firebrand

Hear an industry expert cover the job-ready cyber security skills you should expect apprentices to gain from a vendor-based CREST Cyber Intrusion Analyst programme. Learn how to choose and work with a training provider that ensures your business hires apprentices who can talk and walk cyber.

Jeremy Green is a cyber security and networking professional with almost 20 years of training experience. Jeremy uses his cyber skills and experience in his roles as an IT instructor for Firebrand Training & Apprenticeships, the Army reserves and Derbyshire Constabulary as a special constable.

12:20 – 12:50

Open Discussion - CREST integration into Cyber Security End Point Assessment

John Pritchard, Head of Apprenticeships, BCS & Stefano Capaldo, Managing Director and Co-Founder, Firebrand

This open debate will discuss CREST integration into the new Cyber Security Apprenticeship Standards. The Cyber Security apprenticeship project scenarios taken at end point assessment (EPA) have been written by CREST and count towards two-thirds CREST accreditation/ membership. How do we provide apprentices with full CREST recognition, providing them with the security credentials to firmly align them to a recognised pathway as a Cyber Security professional?

We will be sharing the views from a provider / employer and assessment organisation perspective.

After serving 23 years in the military, John left to establish Smart Computing, a training provider working with Cambridge Regional College to deliver the IT Digital and Professional qualifications and apprenticeships. During that time, he ran national pilots for the introduction of the new User and Technical apprenticeship and was involved in designing new qualifications for the sector. John was awarded the City & Guilds gold medal of excellence for IT and apprenticeship training across the IT sector, as well as, Retail, Finance, the NHS, MOD and Trade Unions. Furthermore, he has since been honoured with lifetime membership to C&G for contributions to educations.

Whilst working with the employers to design the new Apprenticeship Standards at the Tech Partnership John was ensuring employers, providers and Awarding Organisations requirements were aligned to the government regulations to enhance the learners experience, qualifications and competencies whilst beginning their IT careers.

As Director of Learning & Development at Arch, he directed the implementation of the new Apprenticeship Standards and designing the curriculum for delivery to the employers. John now holds the position of Head of Apprenticeships at BCS, working with BCS partners to provide excellence for the Digital IT Apprenticeship Standards.

As Head of Apprenticeships John now leads the team whilst meeting the employers' requirements set in the new Apprenticeship Standards and aligning the end point assessments to meet all sectors engaging in Digital and IT Apprenticeships. His aim is to bring both employers and providers together to ensure the highest quality provision and support can be offered through BCS to support the learners in their career development and closing the existing Digital and IT skills gaps.

Stefano Capaldo is Managing Director and Co-Founder of Firebrand Training. He has worked at the forefront of the IT training and apprenticeships industry for over 16 years, ensuring the delivery of high quality curriculum continues to be the nucleus of Firebrand's apprenticeship provision.

13.50-14.15

Crisis Management – Art or Science

Ian Fish FBCS CITP, Chair, BCS Information Security Specialist Group

Some crisis management gurus claim that crisis managers are born not made. To what extent is this true and how can organisations ensure that they are ready to respond to incidents to reduce the chance that they become crises and respond to crises to reduce the chance that they become disasters while maintaining the ability to respond effectively to events that start as crises or even disasters?

Ian Fish FBCS CITP is Chair of the BCS Information Security Specialist Group and has many years' experience of incident/crisis/disaster management consultancy, training and exercising for organisations in UK central government, the finance sector, transportation, oil and gas, the defence industry and the European Commission. Ian marries this with expertise in cyber security and information privacy by applying system of systems approaches to risk in organisations.

14.20-14.45

Digital forensics and incident response – considering business aspects and legal recourse

Joe Hancock, Cyber Security Lead, Mishcon de Reya LLP

In order to safely realise the opportunities of the digital economy, organisations are looking to develop their cyber risk management strategies and investments, to protect BAU and their reputations in the market. Joe will cover both the business considerations for incident response, e.g. ensuring clients receive appropriate communications of any breach, as well as opportunities via digital forensics to bring the perpetrators to justice.

Joe Hancock is the Cyber Security Lead working within the Dispute Resolution team for Mishcon de Reya LLP. He focuses on providing strategic cyber advice, helping organisations to develop and optimise their investments in cyber risk management, and protect their reputation and stakeholders.

Joe has a wide range of expertise in cyber risk and security, data protection and resilience, with first-hand experience of some of the UK's largest cyber incidents. Through a variety of consulting roles he has helped organisations prepare for cyber breaches and data loss events across global sectors including: Energy, Retail, Defence and Financial Services as well as for government. Joe is a recognised industry expert in emerging areas such as Operational Technology Security and Cyber Insurance. He began his career in the Defence and National Security sector and was one of the first cyber specialists in the Lloyds insurance market, supporting the underwriting of cyber risks.

14.50-15.20

Cyber resilience: current threats and the role of business continuity

Gianluca Riglietti CBCI, Research & Insight Manager, The Business Continuity Institute

According to BCI research on cyber resilience, most of the online threats involve human error to some extent. Using a wide range of techniques, such as phishing or social engineering, cyber criminals can breach into an organisation and cause significant disruptions. Business continuity can help mitigate these threats and ensure a faster recovery. Gianluca will present highlights of the BCI Cyber Resilience Report 2017, looking at the most common cyber attack vectors and how business continuity interacts with other functions of the organisation such as information security, providing insights into how to build resilient organisations.

Gianluca Riglietti CBCI is the Research & Insight Manager for the Business Continuity Institute. He has a Masters in Geopolitics, Territory and Security from King's College London. Gianluca has experience writing academic and industry publications, speaking at international conferences, and delivering projects for companies such as BSI, Everbridge, and Transputec. His previous professional experience includes working for the Italian Presidency of the Council of Ministers.