Chartered Institute of Information Security

Pulse:

December 2021

National Cyber Awards 2021

Results from our live awards ceremony

Dealing with a Breach

Prepare your organisation for a cyber breach

Representing likelihood

Assumptions and issues that lead to error in security

Pulse:

Forward

Welcome

Welcome to the final issue of Pulse for 2021. I hope that your year has been a positive one and that you are moving into winter with an optimistic outlook on the world which many of us were lacking this time last year. With Christmas fast approaching and new year's resolutions coming into play, I am sure we are all looking forward to some downtime to recharge those batteries and to start focussing on 2022 as the year for development, success, and growth.

I would like to take the opportunity to reflect on this year and bask in the accomplishments of CIISec overall, and our internal team. The highlight of this year being our CIISec LIVE event which not only exceeded our expectations as an organisation, but was a hub for innovation, thought leadership and valuable discussions across the two-days. It was highlighted to us post-event that the Career Development Pathways presentation had the highest level of attendance at the event which really resonated with the work that we have been doing to update the ever-evolving Skills Framework.

The synergy between the Career Development Pathways presentation and the uptake of CIISec's Development Programmes following the October enrolments has seen record numbers. We launched the CIISec Apprenticeship Programme (CAP) this year with the aim to provide apprentices with resources and continual development opportunities to help them gain an overall foundation of knowledge to grow within their roles over the 18-24 month apprenticeships. The programme has been well received and we have seen a community of young cyber professionals come together to hear from subject matter experts sharing their knowledge and experiences - all of which has significant impact on bringing fresh blood into the industry.

On the topic of new industry professionals, the CIISec team has grown this year. We have had three new team members come on board in various departments including Jasmin Curtis and Danni Evans both joining the CIISec Secretariat as Membership Coordinators (you are able to get in touch with them both here jasmin.curtis@ciisec.org and danni.evans@ciisec.org). As well as our new Marketing Lead, Elle Pugh – elle.pugh@ciisec.org.

We also took over the running of ICDIP (Institute for Cyber Digital Investigation Professionals) and are delighted to welcome Fiona Paterson into the team. The Institute was created to professionalise Law Enforcement Agency (LEA) cyber digital investigation individuals and has now expanded to private sector investigations. The College of Policing oversee the ICDIP accreditation scheme, which is run by the Chartered Institute of Information Security (CIISec) on a day-to-day basis; with the College owning the skills framework and sitting on the governance board. Please contact Fiona and Marie if you are interested in getting involved icdip@ciisec.org

The theme for this issue is 'Dealing with a Breach' which encapsulates the way that 2021 saw some of the biggest supply chain attacks to date. The impact of these widespread attacks has caused mass disruption to numerous stakeholders and even the public. Within this issue we explore the extreme forms of damage and the ramifications that it brings to organisations. We talk about how purple teaming can prepare your organisation for ransomware attacks, as well as venturing into the Law Enforcement side of how breaches implicate investigations.

As always, do let us know if there is anything you would like to see more from CIISec in the future. We always value your input and your volunteering efforts certainly do not go unnoticed – so thank you! Wishing you a very Merry Christmas, and here is to a prosperous 2022. I hope you enjoy this edition.

Amanda Finch
CEO CIISec

Published by the Chartered Institute of Information Security (CIISec). The views expressed in the articles within this publication do not necessarily reflect those of the CIISec.

No responsibility for any loss occasioned to any person acting or refraining from action as a result of any material in this publication can be accepted by the publisher.

Contents

New Corporate Members

You can find more information on CIISec Corporate Membership www.ciisec.org/Corporate_Membership

SecureAge

We are thrilled that SecureAge have joined CIISec as Corporate Members.

This enables us to collaborate further and to amalgamate our shared values of raising the standards of professionalism in cyber security. We look forward to sharing their thought leadership, helping to develop their teams and welcoming them into our Corporate Member community.

Jerry Ray, SecureAge Technology COO said "Following our UK office opening in 2019, we were excited to become a member of CIISec and are looking forward to share more of our experience in protecting the government bodies and enterprises with the other members. We're also hoping to increase awareness on the importance of tightening company's cyber defence and protecting what matters, without disrupting your work or forcing your employees to become a cybersecurity expert".

To give background as to what SecureAge Technology do, the company places security and usability on equal footing. Headquartered in Singapore, SecureAge are trusted by governments, research institutes, and forward-thinking organisations to protect them from the most advanced cyber threats. What makes SecureAge different is that they have built a reputation for data-centric and intuitive security solutions that do not force users to become cybersecurity experts. That's why their users escape data liabilities and enjoy 100% file-level security, every file, and every time.

For more information about SecureAge please visit www.secureage.com

SecureAge

Apache iX

We are delighted to welcome on board Apache iX.

CIISec CEO Amanda Finch has said "We are looking forward to raising the standards of professionalism in cyber security together through knowledge sharing and collaboration".

For context, Apache iX are a UK wide engineering, technical and specialist P3M consultancy. Their expertise is in strategy and portfolio management; PMO; business analysis; DevOps; and Cyber & InfoSec continues to assist government and industry clients across the defence and security sector with their most complex problems. We support clients to deliver change at all levels throughout the change lifecycle to ensure that client operations and their workforce are empowered, resilient and responsive to the complexities of the Digital Age.

Director Andrew Page at Apache iX has expressed that the organisation is "very pleased to become a CIISec Corporate Member and join others who are making a positive impact in the InfoSec sector. We are delighted to engage with a professional organization of this calibre and contribute to its innovative and purposeful activities and events. We also look forward to sharing with and receiving knowledge from other Members at a time when information security has never been more relevant and vital to personal, national and international security".

For more information about Apache iX please visit www.apacheix.co.uk/

iX

New CIISec Full Members

Congratulations to the following individuals who have recently been awarded Full Membership:

David Harding
Shwetank Juneja
Martin Nash
Christopher Holt
Kathryn Bell
Stephen Duggan
Jonathan Whitehead
Sean O'Sullivan
Dan Harte
James Henry
Farid Khan
Stephen Trenaman
Brett Blackbeard
George Mudie
David Osen
Brian Scobie
James Turrell

New CIISec Fellows

Ken Allan

Independent Information Security Consultant

I have been involved in the information security industry for many years and have worked all around the world on so many different projects large and small. During that time, I have been privileged to have worked with some wonderful people, some of whom are also Fellows of CIISec so to be invited to become a Fellow feels like an endorsement from peers and something I'm very proud of. I can only hope that I can play my part in encouraging, supporting, and coaching others on their own journey.

Simon Moffatt

Founder & Analyst
The Cyber Hut

I have been a member of CIISec for a number of years and before that the IISP. The need for a chartered body was essential for developing the profession and creating a foundation of understanding, knowledge and information sharing. I have been fortunate enough to have worked in the cyber security sector (or information security for the old school like myself!) for over 20 years, specifically within identity and access management. It has been fascinating to see it change, but also how fundamentally more important data security, integrity and availability has become for the modern enterprise, the distributed worker or the digital native consumer. It is everywhere. It is essential. I love the sector and trying to make a difference to the security and usability of our everyday lives. Becoming a Fellow was a great privilege and I hope to take the title to promote awareness and enable the next generation of practitioners to advance the industry further for the next 20 years.

Geraint Jowers

Head of Technical Security at HMRC

My CIISec journey began in 2009, with the then IISP, where I joined as an Associate Member. It was a welcome discovery that unlike other professional bodies, for example BCS and IET that CIISec was solely dedicated to Information Security. In 2010, whilst a CLAS consultant, I applied and was awarded ITPC and by the end of that year I successfully awarded my full membership. In 2013 I enrolled in the NCSC CCP scheme where I obtained both Senior SIRA and Senior Security Architect certification. Joining the ranks of the CIISec fellowship community is a very proud moment for me given the high standards and rigour required in obtaining, keeping, and progressing through the various CIISec membership levels. I sincerely thank those who have contributed and to those who continue to do so in making the Institute such a huge and respected success.

Niall McElroy

Principal at Cydea

Like many of my industry peers, I didn't follow a conventional path straight into cyber security because there simply wasn't one for a long time. Being asked to chair security working groups as a project manager in the MoD was probably my first step of many towards what is now a full-time role in cyber security, where every step since has been more exploratory than planned. I believe CIISec plays a pivotal role in the professionalisation of our industry, setting relevant standards so that people joining the industry now can benefit from 15+ years of formalising the skills, knowledge, and role frameworks that CIISec makes available to all of its members.

Becoming a CIISec Fellow the process requires a nomination by either a CIISec Director or either a Full or Fellow member. If you are interested in learning more please contact **accreditation@ciisec.org**

CIISec STUDENTS OF THE YEAR 2021

Meet the class of 2021 and read about their work, experiences and hopes for the future.

Alex Drane

Best Project
Anglia Ruskin

What was your motivation for studying cybersecurity?

After attending a presentation on cyber-crime and ethical hacking by the Eastern Region Special Operations Unit of the Police I became intrigued by the diverse nature of the cyber security sector, from penetration testing to national security. I was struck by the importance of cyber security to the everyday operations of organisations and the country. With my ambition to help create a better world, I was inspired to aim for a role in this sector.

What was your motivation behind your project?

After studying the methodology of cyberattacks used by malicious actors in an Ethical Hacking module, I was fascinated in ways to mitigate the early reconnaissance of vulnerabilities on a target system. The Ethical Hacking module introduced scanning tools, like Nmap, used for target reconnaissance and enumeration. Experiencing the use of these tools on a live penetration test of a server in a virtual environment allowed me to learn how attackers would act. Here, I utilised stealth techniques to scan the server and successfully find a vulnerability. Consequently, I could exploit the vulnerability to gain root access on the target system. With this experience, I was inspired to investigate ways to mitigate stealth scanning of system vulnerabilities.

Aspirations for the future?

My short-term plans are to enter a graduate cyber security position in an area such as incident response or penetration testing, and eventually progress onto a cyber security master's degree at King's College London or Royal Holloway. A long-term aspiration would be to work toward my dream job of a role in national intelligence or national security at GCHQ or similar organisation.

Deepak Singh

Best Student
Manchester Metropolitan

What was your motivation for studying cybersecurity?

I've always been intrigued with cybersecurity; you can always hear in the media how vital cybersecurity is to businesses and how detrimental it can be to ignore it. Therefore, I've always been interested in what skills I could gain to improve how I write my code to take this into account. I started studying cybersecurity by following some online courses that went over different topics, from network security to penetration testing.

What was your experience with the degree programme like?

The experience was invaluable. As I am studying the Computer Science course, I learned how to become a better programmer in my first and second year and understand the theoretical concepts behind computer architectures, the internet, and operating systems. In my third year, due to my interest in cybersecurity, I decided to choose the information and network security module, which went over a series of topics such as security mechanisms, cryptography, network authentication, access control and firewalls. This was highly beneficial, as it applied over a series of topics I learned in the previous years; therefore, I could use my knowledge from the first two years and understand and apply the topics I learned within the cybersecurity module.

Aspirations for the future?

Now, I have secured a graduate role as a graduate software engineer, and I'm delighted with my position. I plan to contribute by applying the knowledge I've learned during my degree course to develop efficient and robust software whilst learning new skills to become a better programmer. In the future, I'm planning to progress in my current role, and I am also considering completing a postgraduate degree course, either a taught course or a research course, where I could apply my blockchain experience from my third-year project.

CIISec APPRENTICESHIP PROGRAMME

The CIISec Apprenticeship Programme (CAP) has been underway since October and has already attracted apprentices from over 10 organisations. The biweekly webinar sessions have covered key cyber skill areas such as Threat Intelligence and Risk Management.

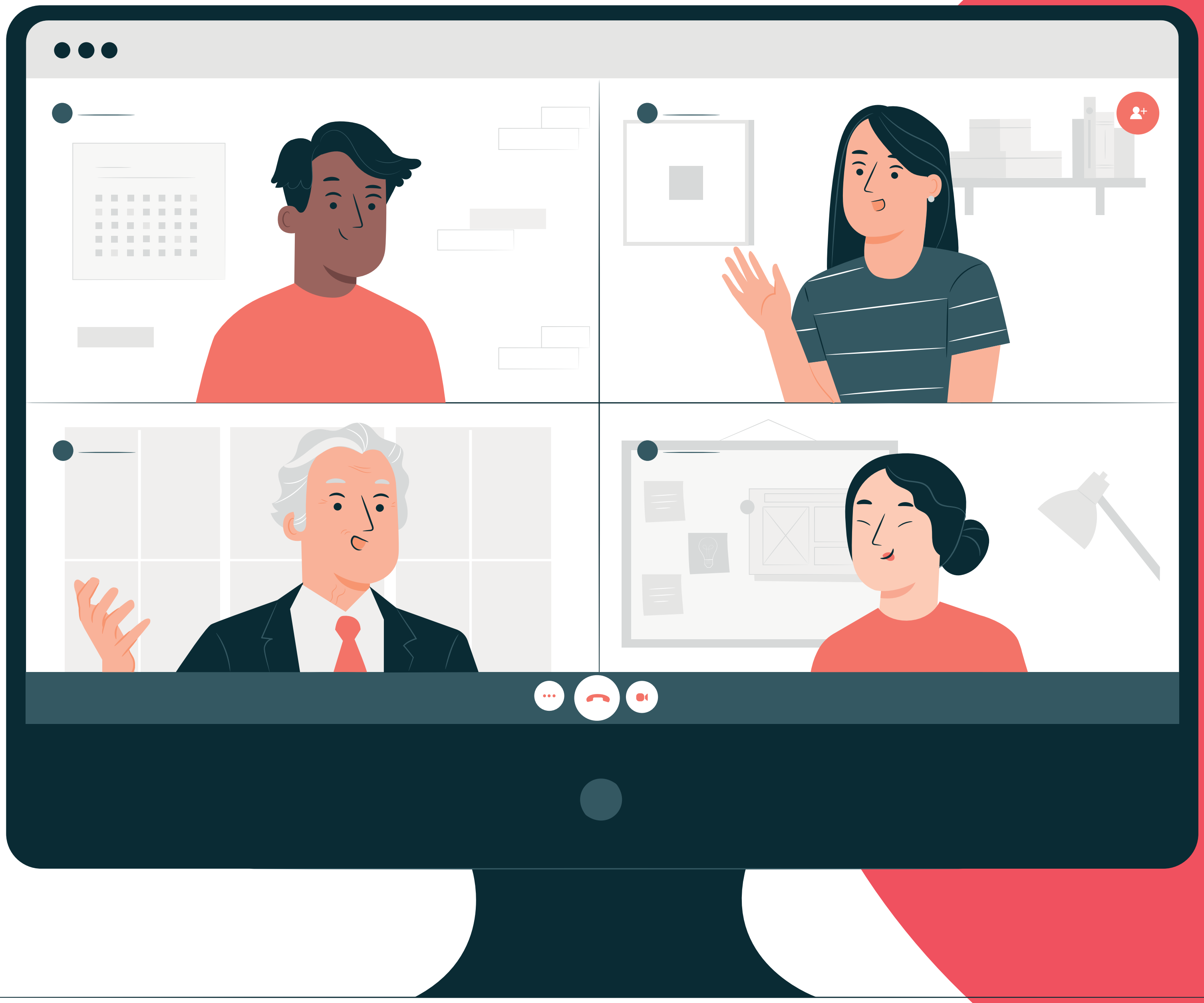
In 2022 participating organisations and their apprentices will have the opportunity to suggest areas of interest they would like to see added to the tailored apprenticeship programme. These tailored sessions will include tips on how to successfully pass their End Point Assessments as well as advancing in their career afterwards.

In addition to providing a packed enrichment programme for apprentices, CIISec is also working on developing a simple "How To" guide for organisations that may be interested in taking on apprentices. This is to support our offerings to businesses to ensure that the onboarding process when taking on apprentices is simplified.

> I just wanted to say a big thank you for all of the CAP Webinars so far, I have thoroughly enjoyed each one and the guest speakers have all been fantastic"

If you are an apprentice, organisation running apprenticeships or would like to host a session, then please email

apprentices@ciisec.org



LIVE CIISec 2021 VIRTUAL

CIISec LIVE 2021

2 Days

3 Streams

80+ Speakers

1,000+ Delegates

Earlier this year on September 15th and 16th, the inaugural virtual CIISec LIVE event took place via our bespoke online platform. It is fair to say that the event was jam packed with thought-leadership content which encompassed both educational features, as well as leading thought-provoking, innovative discussions.

Over two days, three streams, 80+ globally recognised speakers and 1,000+ delegates; the event was incredibly well received by all manner of attendees. The feedback we gathered post-event was truly overwhelming with individuals describing their experiences as:

> Great event., well organised, strong list of speakers and thought provoking.”

> The event was incredible. Given the circumstances we are in, to get a virtual conference right takes a lot of effort and careful planning. It was clear this was done and a lot more. I loved the creative ways to get people engaged and how simple it was to navigate and find where to go next. Really great job and looking forward to the next one!”

With the aim of the event to spark innovation and knowledge in Cyber – we did just that! The event was able to connect information security professionals from across the globe to engage them in a variety of topics focussed around three carefully curated key tracks:

- **Tomorrows World**
  Future Skills and Research Solutions.
- **Digital Disruption**
  Security on The Front Foot.
- **Innovation to Investment**
  Solutions for Emerging Requirements.

We were lucky enough to be joined by globally recognised Keynote Speakers who took over all three tracks on day one and day two with the aim to provide the latest in cyber security innovation and solutions from around the world.

Our panel of Keynote Speakers included:

- **Bruce Schneier**
  Public-interest Technologist.
- **Phil Venables**
  Global CISO, Google Cloud.
- **Steven Furnell**
  Professor of cyber security at the University of Nottingham.
- **Chris Gibson**
  Executive Director at FIRST.
- **James Hadley**
  CEO and Founder Immersive Labs.
- **Ofer Maor**
  Co-founder and CTO of Mitiga.

We wanted to ensure that the presentations delivered across the two days were readily available post-event for those that may have missed sessions, or equally, for those who wanted to go back and re-watch their favourite presentations. Therefore, the content is now live on our YouTube channel for CIISec members, as well as being available via the members area of the CIISec website very soon.

We will be returning for 2022 with a Hybrid approach to CIISec Live. After reflecting on attendees' feedback, we realise that we can accommodate a larger number of delegates and speakers from all over the world with the virtual approach, as well as the benefits of fostering the community through a physical event - it only seems right to blend the two.

We would once again like to thank all of those involved with the planning, preparation, and delivery of CIISec Live 2021. Your generosity, time and effort does not go unnoticed. Watch this space as we prepare for next year!

> The online event was really impressive, top marks and well done to all those that made it happen. Really innovative of the institute”

If you happened to miss the event and would like to dip into a selection of the sessions, here are some suggestions:

DevSecOps: Success Stories

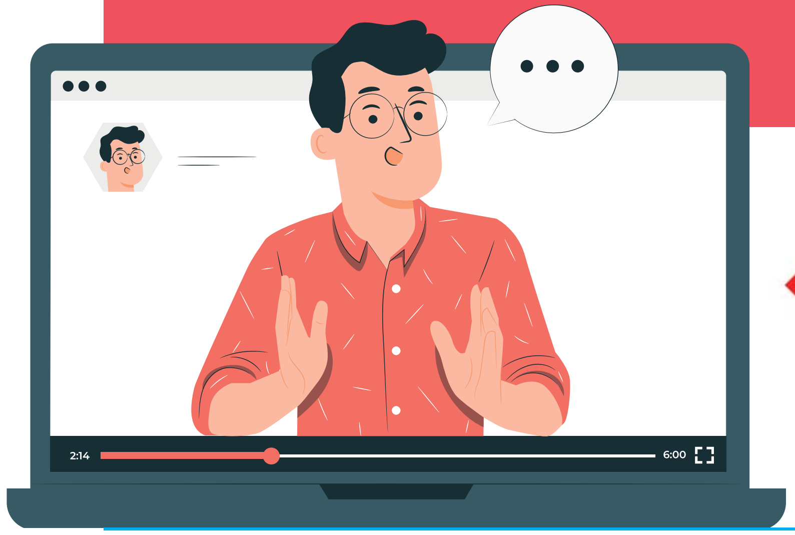
This session was run by Moderator Indy Dhami (Associate Partner - Cloud & Cognitive Security, IBM) and Simon Minton (DevSecOps lead at Deloitte). Through working on large transformation projects, we've seen how organisations can successfully implement DevSecOps practices at scale. In this session, we looked at how organisations are adapting organisational structures to evolve their ability to innovate. We also saw how they are optimising processes & workflows to accelerate time to market, as well as embedding security into their development pipelines.

Data Ethics Panel

Joined by guest speakers from Law Enforcement, Academia, and the College of Policing, guest speakers Dave Lewis, Russ Hinton, Giles Herdale, Dr Carolyn Ashurst and Sarra Fotheringham debate the fact that Law Enforcement are dealing with an increased volume and complexity of digital data with reduces resources. As a result, Law Enforcement are utilising technology, big data, data analytics and AI to support policing and its investigations. However, some officers are worried about the legal implications of exploiting this data, ethically, and are concerned about a lack of guidance in this area.

Development Pathways

Within this session you will hear from Katie Watson, Sophie Baker, Kevin Streater and Richard Lester who will talk you through the structured programmes to support you or to get your team members to the next level as soon as possible, whether you are entering the profession as an apprentice, a graduate, or even changing jobs! This session happened to be the most viewed across the two days of CIISec Live.



LIVE CIISec 2021
VIRTUAL

National Cyber Awards 2021

THE NATIONAL CYBER AWARDS

On Tuesday 28th September the National Cyber Awards took place as a physical event in London with CIISec co-sponsoring the event as well as sponsoring an award for those who have developed and promoted the cyber and digital investigation profession.

The National Cyber Awards is an imperatively placed event to reward those who are committed to cyber innovation, cybercrime reduction and protecting citizens online.

The Nominees

Through much deliberation, the nominees for the award from an Institute of Cyber Digital Investigation Professionals (ICDIP) perspective:

Mike Andrews

National Coordinator of National Trading Standards eCrime Team.

Mike has always been a big supporter of ICDIP since its inception; being one of the first full time members of the scheme, assessing and interviewing candidates, as well as sitting on the Accreditation Committee.

Sarah Montague

Assistant Director Cyber and Digital Forensics at HMRC.

Sarah has been a strong advocate of what the ICDIP do from the early days of the scheme both personally and in terms of promoting ICDIP within HMRC. Sarah also sits on the ICDIP Executive Committee.

Ben Findlay BSc (Hons)

MSc PgCL THE FHEA MBCS MCSFS MIScT MCIIS

Course Leader Computer and Digital Forensics at Teesside University.

Ben is an ex-Investigator of North Yorkshire Police and a full member of ICDIP, who has assisted with reviewing the framework, being an assessor, and has recently successfully guided the first student candidate through the scheme.

Lee Morton

Detective Superintendent, Kent and Essex Serious Crime Directorate.

Lee was a tremendous support in the establishment of ICDIP. Lee acted as an assessor and is also a member of the Accreditation Committee.

The Winner

Jonny Blackwell

Assistant Chief Constable Cumbria Police

Jonny is the most senior ranked member of the ICDIP and is a proactive, vocal supporter of the Institute of Cyber Digital Investigation Professionals (ICDIP), as well as taking a hands-on approach as an assessor and interviewer for the scheme.

The awards will be returning on **26th September 2022**

In addition, many ICDIP members and SPOCs were nominees and winners for other awards presented on the night and it was great to catch up with everyone face to face rather than virtually.

You can find a full list of winners here
www.thenationalcyberawards.org/2021-finalists

DEALING WITH A BREACH

Throughout 2020 and 2021 we have seen organisations adapting to new working environments. With an increase in hybrid working post-pandemic, this has changed the dynamic of cybersecurity set ups globally.

With data breaches happening all too often, organisations of various stature have put their intellectual property in jeopardy, which in turn suffers reputational damage, as well as monetary loss. In this issue we explore the hard-hitting evidence behind cyber breaches during Covid; and how organisations respond by putting contingencies in place to prevent these attacks. We also gain intel from industry experts who delve into the new and innovative ways of working to ensure the safety of organisations and civilians alike – we strive to be proactive to breaches, not reactive when they occur.

Dealing with a Breach

A Security Breach is the Unauthorized Access to an Organization Structure(s) to gain access to Systems, Data, Information, Resources, etc. to carry out Cyber Criminal Activity, affecting the CIA triage and in some cases, operational safety.

Edward Millington BSc, CISSP, ISSA, MCIIS, MIET, PAN-ACE

Cyber Security Consultant | Enterprise Security Architect

Depending on the classification of a breach, in its extreme form, can be damaging to an organisation.

The organisation can suffer:

- Large Financial losses
- Reputation damage – causing loss of interest and viability to Shareholders, Investors and the Public
- Poor Quality and or Availability of Service(s)
- Etc.

In addition, a breach can also affect the safety in operations of the organization and to its Customers. Examples of how a breach can affect the safety of operations and to people are highlighted in the hyper-links below:

www.cshub.com/attacks/articles/another-cyber-attack-affecting-water-supply

www.reuters.com/article/us-usa-cyber-florida-idUSKBN2A82FV

The period between the start of an Incident to an awareness of such an Incident is called the Dwell Time. So it is key to have all the necessary Security Controls (Level 3-4 of the Cybersecurity Maturity Model Certification framework or many of the CIS Controls v8 Implementation Group 3 Controls, where applicable) in place with Continuous Monitoring and Reporting to reduce this dwell time.

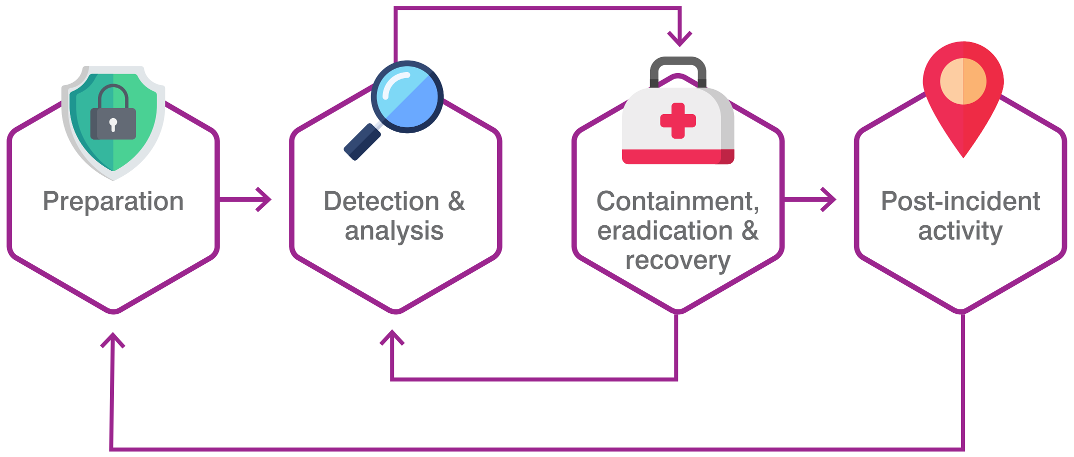


Figure 1

In any event, time is CRITICAL - implying an immediate response is needed to halt and/or minimize the effects and attack surfaces of a breach, especially if it is ongoing - once identified.

In the event of a breach, the organization will activate its Cyber Security Incident Response Plan (CSIRP), taking it through the following phases in the handling of the breach as shown in figure 1.

Preparation

This phase refers to the activation of the CSIRP, which will guide the Cyber Security Incident Response Team (CSIRT) and other Stakeholders in the Communications, Methods of Troubleshooting, Resources needed, etc. throughout the Life Cycle of the Incident Response. All members of the CSIRT should be very familiar at this point with the CSIRP through Table-top exercises, Tests and Reviews.

Detection & Analysis

In this phase, detecting an Incident that can lead to a breach is crucial and can be determined by the notification of an Automated Incident Response System - which correlate Logs from multiple resources (Web, DNS, Hosts, IDS, Firewalls, etc.) to trigger an alert, a Managed Service Provider, an Employee, a Customer, State Authority, etc. These channels will lend itself in the possible determination of the **Attack Vector** used and **Surfaces** affected, which is very important in the analysis and handling of the Incident. An effective designed Information Security Program with a developed Culture of Security will benefit and enhance this Phase.

To handle a breach efficiently and responsibly as possible, a business should express interest in retaining the services of an experienced Incident Management Company or Consultant.

Vectors can be:

- Business Email Compromised
- Infected Email
- Rogue Web Site
- Infected External/Removable Media
- Exploited Application
- DDoS Attack
- Compromised User
- Dissatisfied Employee
- Loss of a Computing Device
- IoT device(s)
- Third Party Access

Once the detection of the Incident is well determined, the next process is the classification and ranking of the Incident in relation to its Impact to a System(s), Data and Information, and Recoverability. Once **classified**, **rank** and **prioritized**, the incident is handled and driven by the CSIRP and its PROCEDURES.

The plan also offers guidance in whether the BCP/DR Plan is activated, the activation of the Forensic Process and how the management of the Incident should be handled in further phases of the Incident Response Life Cycle.

Investigation, Containment, Eradication, Recovery & Notification

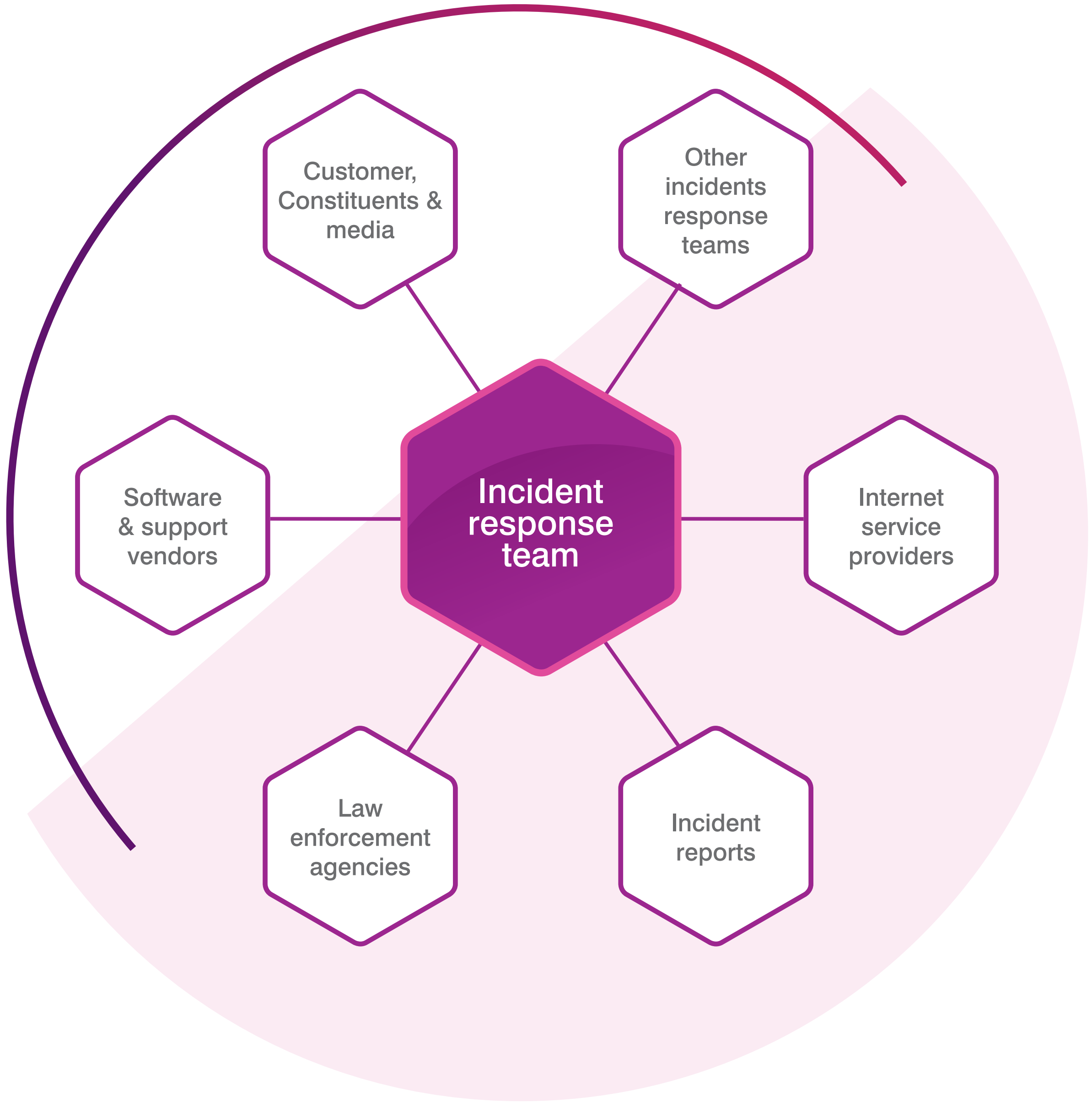
In this phase of the Incident Response life cycle, investigating the incident is critical and it is worthwhile to perform good Forensics best practices, if a Forensic Investigation is needed due to the Operating Industry/ Jurisdiction/Regulation(s) including Legal Criminal Investigations. This is also very important as you move onto the next phase of Containment, protecting the environment (forensically) for legal reasons.

The activities in containing the breach is determined by the type of incident - guided by the CSIRP. That is, the disconnection/isolating of a compromised host(s), redirecting an attack, halting of a Service or Function, etc. This phase is very important in reducing the harm or damages caused by the threat actor.

Damages can take the form as:

1. Encryption of files on a host to network shares
2. Exfiltration of large amount of data
3. Interruption of Systems causing widespread outages or reduce quality of services
4. Damaging or critically affecting Production Equipment
5. Causing unsafe scenarios in relation to people. Example Elevators, Traffic Lights, Water Filtration Systems, etc.

The above are just a few examples when a breach continues due to the slow response of the CSIRT or long Dwell Times.


Customer, Constituents & media
Other incidents response teams
Software & support vendors
Incident response team
Internet service providers
Law enforcement agencies
Incident reports

The Eradication/Recovery/Remediation phases are very important in the repair and prevention to a breach. The processes involve below, but not limit to, can occur:

- Removal of Malware from compromised systems
- Application(s), device(s) are patched
- Physical removal of an Entity from location
- Systems States/Configurations are returned to previous secured operational states
- Hardening of Servers and devices
- Updating of Firewall Policies
- Strengthening of User Access Controls
- Network or Systems changes
- Discontinue of obsolete systems and or software, if applicable
- Removal of unsanctioned software
- Recovered from verified backups

Recovering systems should be verified and monitored to demonstrate secure operations for validation for business functions, processes and capabilities The notification of a breach is very important to the Organisation, Customers, Public, Media, Legal and Regulatory Bodies. It is very important that the notification process activities are carried out by trained personnel, including a Legal and Public Relation Entity - as directed by the CSIRP.

Post-Incident Activity

In this phase, Lessons learned throughout the Life Cycle is critical in responding to future events. Lessons learnt can be:

- The adequacy of the CSIRT Response Times
- CSIRT Incident Response capabilities and knowledge
- The effectiveness and efficiencies of Incident Response Procedures
- The adequacy of communication channels?
- The effectiveness and efficiency of Security Controls implemented
- The adequacy of the precursors and indicators for detection
- The resilience of business processes and technology
- The adequacy for Awareness training for employees to detect and report anomalies

In addition, this phase also include the Retention of Evidence for business and possible Legal proposes. The Retention of Evidence should be guided by a Retention Policy, adhering to your Jurisdiction, Regulation(s) and or Business Legal Policies.

Recommendations

- Business should always understand the impact a Threat will have on it through the use of Risk Management. The critical parts of the Risk Management activities that are very important in the Scope and Impact of a breach is through Asset Management, Risk Analysis, Business and Critical Impact Analyses.
- To handle a breach efficiently and responsibly as possible, a business should express interest in retaining the services of an experienced Incident Management Company or Consultant who would have years and continuing experience in resolving many breaches, especially current breaches, which many internal teams may not have. The entity will have the leadership needed to guide and command the direction of the CSIRT, including the critical communications needed between Teams, Management, Vendors, etc.

To strengthen and enhance the Cybersecurity posture of a business, an experienced Managed Security Service Provider with the ability to work with the business, raising its Cybersecurity Maturity while managing key Security Components should be attained. The key here is to have a well-developed Security & IT Governance Program with Continuous Development, through expert recommendations and advisements.

- Utilised existing standards like the NIST SP 800-61 Rev 2, "Computer Security Incident Handling Guide", NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response", etc. in building your CSIRP and training programs.
- Business should use tools like XDR which correlate data from as many sensors and using AI, Machine Learning and other techniques to alert on Incidents, Risk levels and automated mitigation processes.

48 Percent of UK businesses experience cyber breach during the pandemic

Study by SecureAge

According to a 2021 COVID & Cybersecurity Study commissioned by SecureAge Technology, forty eight percent of businesses have experienced a cyber breach during the COVID-19 pandemic and another 8% 'were not sure'. In addition, 16% of employees said they had personally had to deal with a cybersecurity incident during the same period. SecureAge, a leading global data and endpoint protection company polled 200 employers and 400 employees from around the UK business world during Q3 2021.

"COVID-19 created one of the most challenging periods ever for businesses, their staff and IT departments," said Nigel Thorpe, technical director at SecureAge Technologies.

"A new wave of COVID-inspired cybersecurity threats put the most robust defences to the test and exposed failures in planning, training, tools and overall preparedness. The level of breaches and confusion among employees demonstrates how disorganised and fragmented the cybersecurity landscape has become."

While attacks were targeted specifically at the vast number of people forced to work from home, the SecureAge survey shows that many employers did not provide the level of cybersecurity training to raise awareness of critical threats. Less than 50% of employers that responded said they provided formal training in detecting and handling suspicious emails, password security and protecting sensitive information when working remotely.

"Employers need to deliver more in-depth training or better still, remove the 'weakest link' by taking the human element out of cybersecurity altogether," said Thorpe. "With a recent KPMG survey showing that 94% of workers said they were stressed last year, having one less thing to worry about has got to be a good thing."

> While attacks were targeted specifically at the vast number of people forced to work from home, the SecureAge survey shows that many employers did not provide the level of cybersecurity training to raise awareness of critical threats

66%

Of businesses are set to boost their investment in cybersecurity.

86%

Of employers have already begun to adopt new security measures to cope with the remote workforce.

94%

Of workers said they were stressed last year, having one less thing to worry about has got to be a good thing.

The SecureAge survey also highlights a lack of trust in cybersecurity defences. Only around a third of employers and employees said that they are "very confident" that their cybersecurity infrastructure would protect them from a cyberattack. The pandemic has exposed shortcomings in cybersecurity that are now being addressed. The survey shows that some two-thirds of businesses (66%) are set to boost their investment in cybersecurity, with around 32% of these planning to increase budgets by up to 50%. Meanwhile, 86% of employers have already begun to adopt new security measures to cope with the remote workforce.

"While companies seem committed to improving their resilience, it's important that they spend the money wisely," said Thorpe. "There is an increasing acceptance that it is impossible to prevent every employee clicking on a malicious link or preventing a determined cybercriminal from gaining access to systems and networks. It's time to move away from the 'castle and moat' approach and spending thousands on employee training to take back control with a simple data-centric strategy that focuses on protecting the data itself."

For a full copy of the 2021 COVID & Cybersecurity Study please click here.

For more information on SecureAge please visit **www.secureage.com**

How can purple teaming prepare your organisation for ransomware attacks?

Tom Hall
Head of Blue Team
6point6

Where are we with ransomware?

Ransomware operators and developers are continuously evolving. From their opportunistic roots to the now common Ransomware as a service (RaaS), the effectiveness of ransomware operations has improved drastically.

We're seeing highly effective, targeted deployments, with attack groups conducting operations more like nation state attackers. These attacks span the full attack life cycle including double extortion, meaning that alongside the traditional attack motive of encrypting your organisation's systems, there's the additional motive of stealing your data as well as. Historically, the time from initial compromise to encryption was months, but we're now seeing this reduced to weeks and even days.

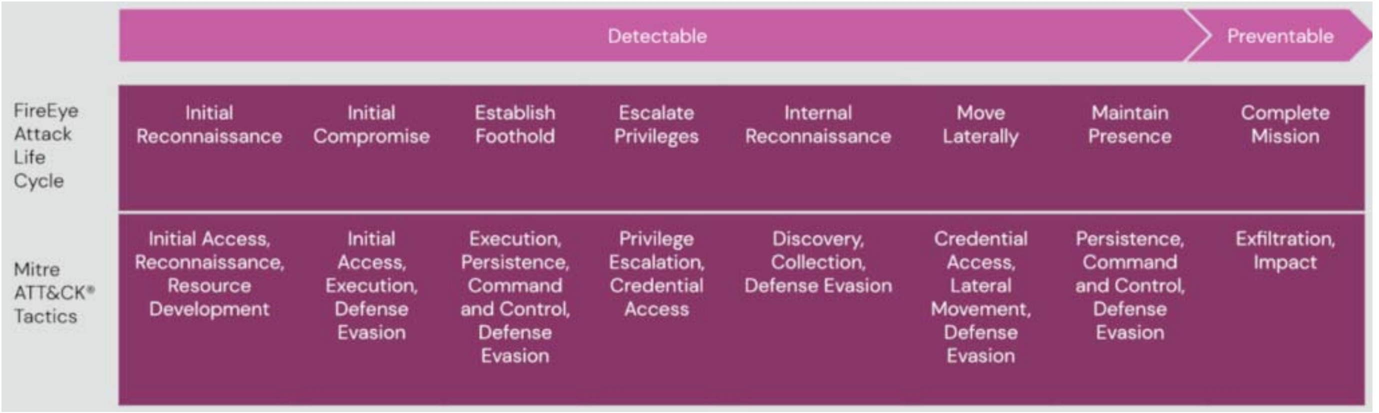
> No organisation can stop attacks from happening, but you may deter attackers by making their job much harder. The less they're able to effectively move around your organisation, the less likely they will be successful.

Detecting attacks early

The goal for an attacker is to cause maximum disruption, and more recently with double extortion, there's the added aim of disclosing sensitive data to force organisations to pay the attackers substantial sums of money.

Ransom attacks aren't going away, but if your organisation can detect them early and prevent the attackers from successfully completing their mission, you can reduce how likely it is for your organisation to appear on ransom demand sites. For ransomware operators to get to the point of stealing data or encrypting systems, there are several steps they must complete. These steps are well described in both the FireEye Attack Life Cycle, and in Mitre ATT&CK® Tactics.

By using purple teaming, organisations can identify where they are stronger or weaker at detecting common attack techniques and build a roadmap to effectively detect activity in this lifecycle.



	Detectable							Preventable
FireEye Attack Life Cycle	Initial Reconnaissance	Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
Mitre ATT&CK® Tactics	Initial Access, Reconnaissance, Resource Development	Initial Access, Execution, Defense Evasion	Execution, Persistence, Command and Control, Defense Evasion	Privilege Escalation, Credential Access	Discovery, Collection, Defense Evasion	Credential Access, Lateral Movement, Defense Evasion	Persistence, Command and Control, Defense Evasion	Exfiltration, Impact

What is purple teaming?

Purple teaming combines technical expertise to ensure a valued outcome for your organisation. It uses elements of red teaming, by assessing your incident response capabilities though simulating real world threat actors and scenarios. But this is done in combination with a blue team, assisted by our experts, to build and develop the capabilities you need to defend against future attacks.

Purple teaming simulates a broad range of threat actor capabilities to determine how effective your detection is. And it includes gap analysis so your organisation can uplift its capabilities going forward.

Are you ready for purple teaming?

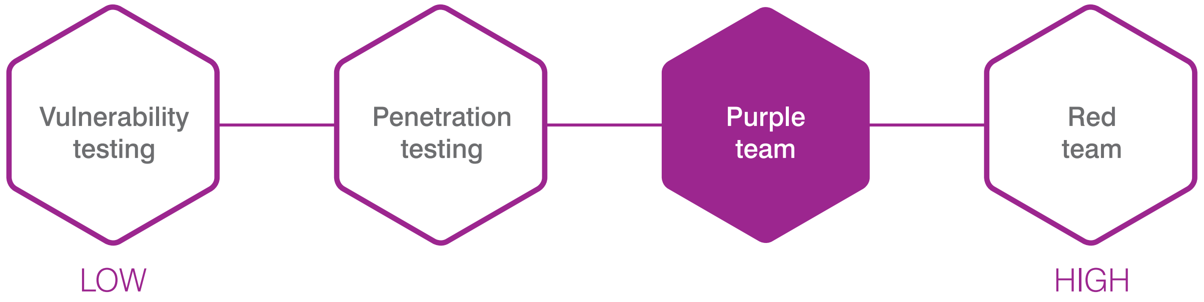
Whether you're ready for purple teaming depends on your organisation's maturity. For example, running a purple team exercise if your organisation doesn't have the basics in place offers little benefit as you first need to have the processes and technologies needed for detection and prevention capabilities in place.

Purple teaming sits between penetration testing and red teaming for effectiveness in organisations. It bridges the gap between them and helps organisations who are in the lower half and middle of the scale.

Preventing disruption is key

Using purple team testing to understand the gaps in your detection and response capabilities, and then uplifting them where possible, means you'll be better equipped to face attacks in the future. No organisation can stop attacks from happening, but you may deter attackers by making their job much harder. The less they're able to effectively move around your organisation, the less likely they will be successful.

Start a conversation
If you want to find out more about how we can help you with purple teaming, please contact Tom Hall on **tom.hall@6point6.co.uk**



Data ethics in policing – challenges and opportunities

This is a summary of some of the issues covered in a panel session at the CIISec live event on 16th September.

Giles Herdale
Herdale Digital Consulting

Organised by Fiona Paterson from CIISec, the panel was moderated by Dave Lewis, formerly the NPCC lead for ethics and Deputy Chief Constable of Dorset police, and featured Giles Herdale, independent expert on digital investigation and ethics, Russ Hinton, a data ethics manager from the law enforcement community, Sarra Fotheringham, policing standards manager for digital and cyber at the College of Policing, and Dr Carolyn Ashurst from the Alan Turing Institute.

> Our policing style is based on legitimacy and our legitimacy is based on trust and confidence of all of the communities. It is a fact that the trust and confidence levels within the black community are 20%, or thereabouts, lower than the white communities, and that [has] impacted on the trust and confidence for us to do what we do as a service.

Data ethics in policing: The challenges and opportunities

We are living in a time of exponential change, driven by a combination of factors including: the technological revolution, the continuing effects of the pandemic, the climate emergency, a new diversity awakening (such as Black Lives Matter and Me Too), and global competition in a multi-polar world (characterised in part by the rise of China, US retrenchment, and Brexit).

These separate, interconnected phenomena are posing significant questions and challenges to societies, their politics and institutions, as well as states, globally, including the UK.

Policing is perhaps uniquely exposed – as the renowned post-war Met Commissioner Sir Robert Mark observed:

The ***police*** *are the* ***anvil*** *on which society beats out the problems and abrasions of social inequality, racial prejudice, weak laws and ineffective legislation.*

> On one level it is impossible to argue against the necessity for law enforcement to embrace technology in order to successfully respond to the changing demands of society

Crisis in legitimacy from several fronts

It has become increasingly clear that the licence to operate for policing is being questioned and challenged. As chair of the NPCC Martin Hewitt said last year regarding Black Lives Matter:

Our policing style is based on legitimacy and our legitimacy is based on trust and confidence of all of the communities. It is a fact that the trust and confidence levels within the black community are 20%, or thereabouts, lower than the white communities, and that [has] impacted on the trust and confidence for us to do what we do as a service.

In this context police legitimacy is constantly being renegotiated, and police use of data and technology is under the spotlight.

Policing technology under the spotlight

Data and technology are at the centre of this. We have seen the power of technology grow during the pandemic as we have become increasingly reliant on it. As tech companies and entrepreneurs have benefitted from this uptake, so scrutiny of technology has increased – fears about privacy drive the advertising campaigns of some tech giants, predictive technologies are increasingly contested, and the industry and regulatory response is characterised by uneven maturity. Above all, data has become central to the power discourse – you may have heard the oft-used saying 'data is the new oil'. Searching questions are being asked about the wider societal benefit of technology services based on harvesting mass personal data – so called surveillance capitalism.

So how does this impact on policing? On one level it is impossible to argue against the necessity for law enforcement to embrace technology in order to successfully respond to the changing demands of society, the threats of changing crime trends, and the need to support victims and witnesses. With policing being a people business, the need for effective engagement to build public trust means that opportunities to develop data capabilities is very pressing.

At the same time, policing is an information business and a prevention business. Police leaders and those who have an interest in safe, effective, and proportionate policing, which should be all of us, should therefore be asking 'just because I can, does that mean I should?' There have been some highly contested recent examples, ranging from the use of social media scraping tools, through the deployment of phone download technologies or use of facial recognition systems, to the deployment of drones to support enforcement of pandemic related restrictions.

This is raised not to pass judgment on any of these cases, but to highlight the importance of a rigorous assessment of costs, benefits and impact during the development and pre-deployment cycle. The importance of good governance and ethical decision making processes is key to the successful use of technologies, especially considering the inevitable scrutiny that policing will face.

The temptation to argue that 'everyone else is at it, so why shouldn't we?' doesn't really pass muster here. Policing has always been the subject of intense scrutiny and, rightly or wrongly, held to a higher standard, because of the nature of the exceptional powers and trust placed in the office of constable. Maintaining and building that trust is the key to success for policing in the future.

Building a coherent response

It is therefore encouraging that there is growing recognition of the need for more systematic attention to the process of authorising development and deployment. This has been highlighted in the Policing Vision 2025 and the recently published National Police Digital Strategy.

This is a newly-emerging field and maturity levels are still quite mixed across the policing landscape. Pockets of good practice have developed (West Midlands Police, the NCA, Essex and Police Scotland all deserve a mention in this regard). But it can be argued that this is despite, rather than because of, central organisation or guidance. Clearly there is a need for greater co-ordination and leadership in this space. The NPCC have recognised this and CC Richard Lewis, who chairs the UK Police Ethics Guidance Group, is setting up a digital ethics sub-committee. The College of Policing is reviewing the existing Code of Ethics, (recognising that data ethics must play a part) and have started issuing guidance on issues such as mobile phone extraction and facial recognition.

Hopefully in coming months this work will develop further, and will be integrated into leadership development programmes. There is a growing demand for digital leadership and the development of data literacy amongst the workforce. This has seen some consideration of how to train staff, one example being a data ethics programme designed for senior leaders that we have developed with Enlighten Training.

> Everything suggests that this is the time for policing nationally to step up and coordinate a comprehensive, joined-up approach to the challenges of new technology.

Although policing is very much under the spotlight it is not alone in facing the challenges of navigating the complexities of this digital landscape. There is a growing body of expertise across academia, industry, civil society, and government that can inform and support law enforcement agencies. In particular, the work of bodies such as the Alan Turing Institute (the UK national centre for data science and AI), the Centre for Data Ethics and Innovation (an independent expert advisory body established by Government), and the Ada Lovelace Institute (a civil society research organisation that is examining the impact of data and technology on society) is directly relevant to the development of a policing data ethics framework.

The stars are beginning to align, with a developing emphasis on technology harnessed for public benefit, increasing public scrutiny and challenge, and a forthcoming spending review. Everything suggests that this is the time for policing nationally to step up and coordinate a comprehensive, joined-up approach to the challenges of new technology and demonstrate responsible and ethical innovation. Only by doing so, and in such a way that reinforces public trust in police use of data and technology, will the law enforcement bodies that keep us safe be able to harvest the benefits of this exciting, but hotly-contested future.

Published through:
www.policinginsight.com/features/data-ethics-in-policing-the-challenges-and-opportunities/

Meet Fiona: The ex-cop helping CISOs nail hackers

With a 17-year career in the police force, former investigator and all-round cyber action woman Fiona Paterson has form in whodunit cases.

Author
www.insight.scmagazineuk.com

Now she's focused on rooting out hackers in big business and the wider landscape – leading the world's first cyber investigation accreditation programme for detectives, analysts, legal and IT staff.

Fiona Paterson has spent over two decades trying to get to the bottom of things. With a background in forensic psychology, her lifelong fascination with human behaviour has supercharged her career in crime detection and rooting out cyber fraudsters.

"My former chief constable used to call me a 'computer dweller' because I was one of these people that sat in a room as an analyst and knew how to get information out of computers," she says. "When I worked for Sussex Police, I noticed more investigations becoming based around people using social media or the web.

> Specialist police units spend a lot of their time focusing on breaches to small businesses or big corporations, especially ransomware. Large-scale fraud and cryptocurrency scams are on the increase.

So it was just having an interest in human behaviour that drove me to learn how online investigations work."Paterson's keen eye for cyber analysis soon saw her leading a national police working group and going on to work for the Bank of England (BoE) "working to prevent a cyber attack from collapsing all the banks", she says, as if it was all in a day's work.

Making sure cybercrime doesn't pay

But the pull of law enforcement drew Paterson back to the College of Policing (CoP) this year to help launch the Institute of Cyber Digital Investigation Professionals (ICDIP) – the world's first organisation to benchmark skills for cyber investigations.

ICDIP measures the competency of practitioners, allowing them to prove their expert status and speed up the professionalisation of cyber digital investigations. Ultimately, ICDIP will aim to increase trust in digital evidence, give greater weight in court cases, and to help ensure fair convictions. What's more, CISOs now have a welcome tool in their cybersecurity armoury kit – the ICDIP can accredit corporate types, such as analysts, researchers and general counsels, as well as law enforcers. Originally a Home Office project, the ICDIP is now managed by CIISec (Chartered Institute of Information Security).

"When we launched five years ago, we were really focused on dedicated police units but we soon found that nearly every crime has a cyber or digital element – about 97 to 99 percent of the time," says Paterson, now programme manager for CIISec and a former project lead for CoP.

Anyone can buy ransomware tools on the dark web

According to the former detective, corporate malfeasance comprises a large part of cybercrime. Specialist police units spend a lot of their time focusing on breaches to small businesses or big corporations, especially ransomware. "Large-scale fraud and cryptocurrency scams are on the increase. When I worked at the BoE, we used to talk about nation state attacks and how their expertise would take between two and five years to filter down," she says. "Now, information transfer can happen in a number of weeks – it can be a 15-year-old, any criminal can buy ransomware tools off the dark web. It doesn't take a lot of expertise to run an attack."

You'll know a good cybersecurity team when they're gone

Paterson emphasises that ICDIP is not a training course. "It's an accreditation of competency of someone's skills in cyber investigations in their day-to-day role," she says. "Your staff may go on training courses but as a line manager or a CISO you might not know if that person is performing their role to an effective standard. This accreditation is assessed by peers and national experts with a view to strengthening corporate and public safety." The reality is you don't know if you've got a good cybersecurity team until they are gone, says the crime buff. "The amount of times I've heard financial company board members say that cyber attacks 'aren't an issue' for their organisation, so they reduce their budget and the very next day there is a security breach."

I was the lone female among grey men in grey suits

Over a two-decade career, the corporate investigator says she often found herself a lone female amid a sea of middle-aged men clad in grey suits. "In terms of diversity, the cybersecurity industry was not in a good place. But, in recent years, it's definitely improved," says Paterson, who regularly goes into schools to talk to pupils about how cybersecurity can be a fulfilling career for women and men.

"Sometimes people are put off by the technical side of cybersecurity but actually there are lots of interesting roles people can get into," she says. "What's more, the language that is used within organisations – talking in jargon and making things complex – can put people off. So much can be done to improve the language of job adverts and describing the skills and experience you need to get into a role."

Paterson says "having an open mind and being a creative problem solver" can be a solid starting point for a cybersecurity career. "You're more likely to solve a problem with a bunch of people from different backgrounds with different ideas than if you have the same people with the same ideas coming through."

Insider tips: Paterson's cyber fraud hygiene list

Identify company vulnerabilities - The identification of security vulnerabilities – and taking them seriously – is key.

Communicate clearly and widely - Make sure that cybersecurity is something that everyone in the organisation is aware of – it's not just down to the CISOs and the cyber team.

Steer clear of scapegoating - Cyber security is everyone's responsibility but be mindful not to cultivate a blame culture.

For example, if an individual does fall for a phishing attack, it should be about learning from the mistake rather than apportioning blame. If employees or stakeholders are fearful of consequences, they are less likely to report anything that they see as suspicious.

HMPPS Digital Media Investigation Unit (DMIU)

HMPPS' Digital Media Investigation Unit (DMIU) is a specialist team that was formally established at the end of 2018.

Ryan McGovern
London Hub Manager
Digital Media Investigtion Unit
HMPPS

DMIU was set-up to ensure that the 3 key digital tactics: Internet Intelligence & Investigation (III), Communications Data and Digital Forensics could be managed consistently within one Unit to support applicants that require these specialist tactics to be used in order to progress their investigations. DMIU has become a 'Centre of Excellence' in relation to digital tactics being used in HMPPS and was formally recognised for delivering such a high-quality service in 2019, when the team was awarded the title: 'International Digital Investigation and Intelligence Team of the Year' at the annual ICDDF conference, beating 18 other Law Enforcement teams to win this prestigious award. The team's capability and expertise has increased substantially since its inception 3 years ago and continues to grow in line with new and emerging risks and threats that are associated with illicit communication devices being used from within prison custody.

The team's capability and expertise has increased substantially since its inception 3 years ago and continues to grow in line with new and emerging risks and threats that are associated with illicit communication devices

Internet Intelligence & Investigation

DMIU supports prisons, regional and national intelligence colleagues in locating, capturing and requesting removal of social media content that has been uploaded by prisoners from within custody. The team has established and built strong working relationships with the larger social media companies, and looks to engage the smaller; more novel websites on an ad hoc basis. Alongside locating, capturing and requesting removal of illicit content, DMIU also encourages and supports prisons in taking appropriate local action against prisoners whom have misused social media from within prison. This may include contacting the prison if the social media account has been updated recently to try and help retrieve the illicit mobile device being used, or providing advice and guidance on what punitive action can be taken, such as an adjudication or referral to the police.

Communications Data

DMIU has a team of accredited SPoCs, who are able to request and acquire Communications Data legally from Telecommunications Operators (TO) and Postal Operators (PO) under the Investigatory Powers Act 2016, in order to help evidence criminality linked to illicit communication devices that affect HMPPS. DMIU offer tactical support to regional and national intelligence teams, as well as colleagues in prisons, in order to assist and progress criminal-focused investigations.

> The team is also responsible for the extraction of data from illicit devices seized within prisons. The vast majority of devices are mobile phones and related items (SIM Cards / Memory Cards).

Digital Forensics

The team is also responsible for the extraction of data from illicit devices seized within prisons. The vast majority of devices are mobile phones and related items (SIM Cards / Memory Cards). Capability is in place to extract data from these digital devices through using specialist extraction equipment to extract data from locked devices.

Devices are received from across the service and the extracted data is provided to support prison, regional and national intelligence investigations. Support is also offered in regard to utilising specialist analytical software that enables investigators to better interpret the data.

Alongside continuing to manage and support the use of these 3 digital tactics within HMPPS, DMIU has also been on a developmental journey over the past 12 months; specifically, designing, co-ordinating and now looking to implement a wider Digital Media Investigation Capability Improvement Programme.

The first area of this DMI Programme was looking at the 3 digital tactics we are responsible for and identifying – within DMIU - how we can better link all 3 tactics together when supporting applicants carrying out an investigation that has a digital element. Previously, we carried out all 3 digital tactics to a high level individually but did not necessarily encourage or assist applicants in looking to exploit further digital lines of enquiry. Therefore, we have established a set of 'core' questions that we encourage applicants to look at and follow and have also designed internal processes that look at driving the use of all tactics relating to digital investigations. These new processes have been embedded over the past 12 months and we have started to see some positive results from applicants that have used all tactics to drive criminal-focused investigations.

Alongside linking the 3 digital tactics together better, DMIU management have also looked at the wider HMPPS intelligence teams that have been set-up over the past few years, in order to identify how we can raise better awareness of the services we offer to these teams. As part of this, DMIU has developed and is in the process of implementing a Regional Digital Media Investigator (RDMI) network, which consists of a group of staff from these wider regional and national teams being up-skilled and equipped to use digital tactics regularly.

The primary purpose of establishing the RDMI network is to:-

1 Enhance regional and national intelligence colleagues' knowledge and understanding of how to engage with and use these tactics more regularly through setting up bespoke training courses.

2 Equip colleagues with the specialist hardware and software so they can use these tactics effectively at a regional and national level.

3 Enable colleagues to follow a 'Digital Professionalisation Pathway', through achieving ICDIP accreditation to professionalise HMPPS analyst staff involved in digital investigations and to replicate accreditation achieved by all DMIU staff.

> The ultimate aim of this capability roll-out is to embed DMIU's 'Centre of Excellence' into regional and national intelligence teams.

Specifically, this group of RDMIs will be responsible for carrying out Internet Intelligence & Investigations on regional subjects / threats, becoming a 'professional' applicant in relation to applying for and subsequently analysing Communications Data, as well as analysing Digital Forensics extraction reports linked to seized illicit communication devices found in possession of nominals of interest.

The ultimate aim of this capability roll-out is to embed DMIU's 'Centre of Excellence' into regional and national intelligence teams. This process is in its early stages of implementation; staff who are carrying out this role have been formally identified and an Induction Booklet has been sent to all providing an overview of the role and the duties and responsibilities assigned to it. Progress will be monitored throughout by DMIU Managers and support will be provided by the central team to all RDMIs to help them flourish in this role as well as achieve formal ICDIP accreditation.

REPRESENTING LIKELIHOOD REALISTICALLY

Of the two core parameters of risk, likelihood is the least well understood within the infosec risk management community.

Mike Barwise,
Director, Integrated InfoSechip

So I feel it's time to draw attention to some assumptions and issues that lead to error, and to suggest a way forward to improvement.

We can assess likelihood using either a frequentist or a probabilistic representation.

Frequentist assessment attempts to estimate the likelihood of an event occurring on the basis of the expected interval between events: once a month, once a year and so on. It's currently the preferred approach in the infosec community, to the extent that it dominates the guidance provided by international standards and is widely considered to be 'best practice'. This may be because it's easy to visualise without any formal training, but unfortunately it suffers from some failings that make it untrustworthy.

It assumes that events occur with constant regularity. But although courtesy of the statistical Law of Large Numbers[1] the intervals between very large numbers of randomly spaced events tend to a stable average, there's no equivalent 'Law of Small Numbers'. The average interval between small numbers of such events is generally a poor predictor of an individual event occurring. But even for large numbers of events, the average can be uninformative in a given case because the dispersion[2] (the width of the range between the maximum and minimum event frequencies) can be very large, so the actual rate of occurrence at any particular moment may be far from the average. Failure to recognise this all too often underpins a tacit assumption that the clock starts when your project starts. But considering a 'once in ten years' event to be irrelevant if your project or service has a life of, say, a couple of years ignores the fact that the notional rate is only an average. The overlooked 'once in ten years' event could quite possibly occur twice next Tuesday. Dangerous as these assumptions are, the frequentist representation of likelihood has an overriding intrinsic flaw – it prevents aggregation of risk factors.

Nothing happens without causes. Real risk events result from coincidence of typically multiple contributory factors, and the likelihood of an event obviously depends on the likelihoods of its contributory factors.

Dangerous as these assumptions are, the frequentist representation of likelihood has an overriding intrinsic flaw – it prevents aggregation of risk factors.

These combine in strict mathematical ways depending on the logical relationships between the factors, but unfortunately the math doesn't work if we use the frequentist representation. So frequentist assessment can't be based on causality, but can only be plucked from past experience of the totalities of similar scenarios. This can be sufficient in fields such as motor insurance where causalities are relatively simple and unchanging, but the information security landscape is too complicated and too unstable to deliver adequate historical records. Consequently, prediction on this basis will not yield results that accord with reality.

To get nearer the truth, we must rely on the mathematics of probability. But before you cringe in horror, only the basic principles are required, and they're actually quite simple.

Probabilistic assessment represents the estimated likelihood of a single instance of an event occurring within some constant frame of reference – for our purposes usually a fixed time interval – on a scale of zero to one (or, equivalently, zero to 100 per cent).

The fundamental advantage of this representation over the frequentist one is that it allows the use of valid math to aggregate risk factor likelihoods. So instead of having to guess a likelihood for an entire scenario, we can in principle calculate a scenario likelihood from the likelihoods of its contributory factors. The result is increased reliability through improvement in both the realism of individual assessments and the consistency with which multiple assessments can be performed.

In his snappily titled 1853 blockbuster *An investigation of the laws of thought on which are founded the mathematical theories of logic and probabilities*[3] George Boole demonstrated that the fundamental mathematics of probability are essentially the same as the core mathematics of propositional logic – familiar to us as the Boolean algebra[4] used by digital systems designers.

So how do we make effective use of the probabilistic representation of likelihood? Merely assigning notional probabilities to scenarios against a quantised scale won't get us any further than using frequentist assessment. But investigating causalities can hugely improve the quality of results. The first step is to build a 'factor tree' from our risk scenario. This consists of successive tiers of causal factors connected at each level by their logical relationships (Figure 1). In each tier, several factors that must all occur to create an outcome are coupled by logical AND, whereas several alternative factors, any one of which is sufficient to cause the outcome are connected by logical OR. Replacing the logical relationships with the relevant probabilistic equations allows us to calculate the aggregate probability of the scenario cumulatively from the probabilities of its causal factors.

But where's the gain? Provided the factor tree is sufficiently exhaustive – that is, crucially, that we've understood the scenario and its causes well enough – the method massively reduces the uncertainties that render the results of frequentist assessment questionable. Quite apart from the weaknesses already mentioned, when using a frequentist scale we are obliged to slot events into typically quite broad categories of likelihood before any risk calculations are performed. This causes actual event likelihoods that fall somewhere between the defined category boundaries (in practice, almost all event likelihoods) to be variably misrepresented, leading to significant but subsequently undetectable assessment error. The probabilistic factor tree allows a much closer approximation to reality as likelihood values are determined by the relationships between the factors in the tree rather than being distorted by forcing them into a limited number of arbitrarily pre-defined categories.

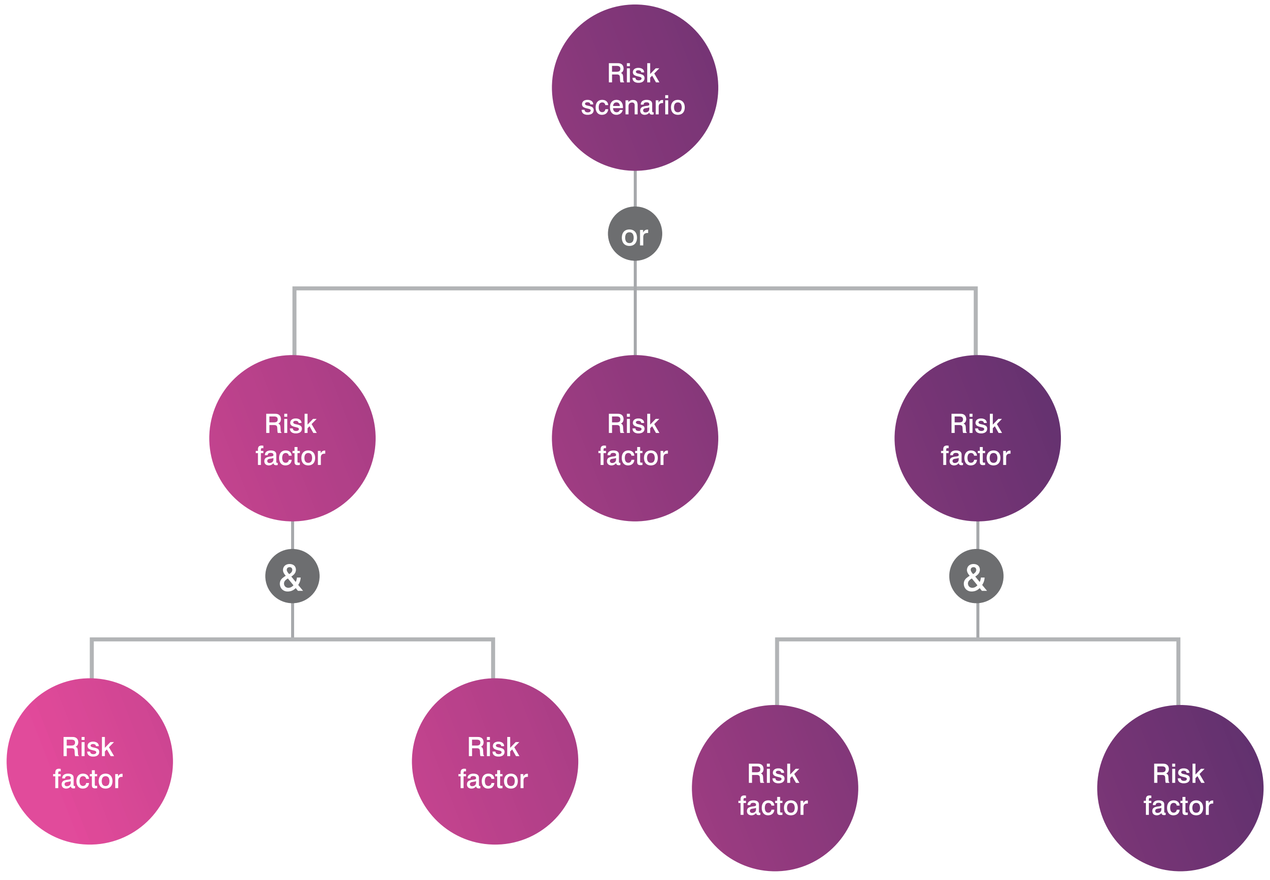


Figure 1 A simple risk factor tree

The bottom line is that reliable risk assessment absolutely depends on understanding and applying the core axioms of probability theory, as these are a formal expression of what actually happens. So to ignore probability theory is to ignore reality. The fundamentals first appeared in ***De Ratiociniis in Ludo Aleae***[5], a pamphlet on the chances of winning at dice published by Dutch polymath and gambler Christiaan Huygens in 1657. Particularly as it's not 'scary math', it's utterly appalling that after three and a half centuries this elementary but crucial body of knowledge still doesn't feature in mainstream risk management practitioner training. For now, learning it is a case of DIY but it's essential. Otherwise, we'll just continue unwittingly generating random numbers while kidding ourselves we're assessing risk.

Mike Barwise is a CCP Lead SIRA and veteran information risk management consultant with a background in systems engineering. He contributes to ISO risk standards development and is keen to collaborate with fellow experts in improving the realism of information risk management and practitioner training.

REFERENCES

1 wikipedia.org/wiki/Law_of_large_numbers
2 wikipedia.org/wiki/Statistical_dispersion
3 www.gutenberg.org/files/15114/15114-pdf.pdf (particularly chapters 16 & 17)
4 www.britannica.com/topic/Boolean-algebra
5 www.sciencedirect.com/topics/engineering/quantisation
6 math.dartmouth.edu/~doyle/docs/huygens/huygens.pdf (English translation 1714)

Dates for your Diary

Paul Schwarzenberger joins us for a Masterclass about AWS, Azure and GCP Security

Date: 13 January 2022

Paul is a cloud security architect and engineer with over 15 years' experience, leading security, and cloud migration projects for customers across sectors including financial services, Government and the energy sector. He has in-depth enterprise experience of all three major cloud platforms – AWS, Azure and GCP. Using live demonstrations, we'll compare security architectures and features for Identity, Private Networking and Content Delivery Networks - across all three clouds.

We'll look at three common use cases:

- Identity: cloud customers typically create multiple AWS accounts, Azure subscriptions or GCP projects. How should a centralised source of identity be architected?
- Private Networking: security conscious cloud customers use private networking as part of a defence in depth strategy - how can this be achieved with cloud services such as storage or serverless functions which are Internet facing by default?
- Content Delivery Network: how can a web application be presented to global users with low latency and a high level of security?

We'll conclude by looking at the implications for organisations considering a multi-cloud approach to security.

Register here →

East Anglia Branch Masterclass – Supply Chain Ransomware: The Looming Iceburg

Date: 26 January 2022

Over the years Ransomware has evolved and adapted to changing regulatory landscapes, inclusion of more sophisticated security tools and advancements in processes and techniques. This has resulted in a potentially perfect storm, supply chain attacks. Exasperated by outdated vendor supplier validation techniques, supply chain attacks have the potential to reach millions of organisations with a single breach. During this session Jason Nolan, and Andrew Yeates from ReversingLabs will unpack the predictions for next generation supply chain attacks, how to get ahead of the curve and protect against them. The session will be hosted by Andy Young, Security Solutions Architect at Keysight Technologies

Register here →

Diversity and Inclusion Panel for ICDIP Women in Cyber webinar

Date: 20 January 2022

Can we have (or balance) it all? Diversity and Inclusion webinar

Date: 22 February 2022

InfoSecurity Europe ExCel London

Date: 21-23 June 2022

Infosecurity Europe is the biggest gathering of the information security community in Europe. Each summer we come together to share innovation, learn from each other, test and benchmark solutions, build relationships and drive new business.

More info →

With the world returning to the 'new normal' we are hoping to collaborate more in person throughout 2022, which is why we have decided to mix up our event programme to be a combination of physical and virtual events. We know that there has been a real excitement around getting back to seeing one another in person so we are extending our offerings to include your wishes on this going forwards. Equally, we understand the benefits of hosting virtual events as they have allowed us to collaborate in a way that we once wouldn't have. We have brought together a global array of speakers to our webinar programmes and wish for this to continue for our members to enjoy and be involved in.

We would love to hear your thoughts on events in 2022, so please do get in touch with us to let us know what you would like to see more of from CIISec in the future.

About The Chartered Institute of Information Security

The Chartered Institute of Information Security (CIISec) is the only pure play information and cyber security institution to have been granted Royal Charter status and is dedicated to raising the standard of professionalism in information and cyber security.

CIISec provide a universally accepted focal point for the information cyber security profession, it is an independent not-for-profit body governed by its members, ensuring standards of professionalism for training, qualifications, operating practices and individuals. CIISec has a growing membership that represents over 20,000 individuals in the information and cyber security industry.

Evesham Office
Haddonsacre
Station Road
Offenham
WR11 8JJ

London Office
CAN Mezzanine Borough
7-14 Great Dover Street
London
SE1 4YR

www.ciisec.org

Chartered Institute of
Information Security