Information Assurance Advisory Council

IAAC

The Profession

Understanding careers and professionalism in cyber security

IAAC is sponsored by:

O2 gsk Reliance acsn Specialists in IT Security Management sopra steria QinetiQ BT

FORTINET NEXOR Ultra ELECTRONICS NORTHROP GRUMMAN Detex

Contents

Executive summary

1. This report is the result of four workshops, drawing on the expertise of the IAAC community, many of whom contributed their personal time, together with IAAC's own desk research. It provides a narrative regarding the profession, aimed at an audience from careers advisers to prospective employees and professional bodies. The report defines the context and the nature of the challenge regarding the Profession. It outlines the research approach. The themes that emerged are explored and discussed before recommendations are made.

2. IAAC **recommendations** are as follows:

a) Professional bodies and any new initiatives under consideration should review the principles of a profession, set out by Lord Benson in his 1992 speech (see below)
b) It is unlikely that there can be a single professional body for everyone professionally involved in cyber security. It might be better to talk about a **profession of professions that work together to manage security and mitigate risk** (i.e. a 'meta-profession').
c) As a meta-profession, the core skills of the professional would indicate their base professional association, though they may need to belong to more than one body depending on the role they are fulfilling in a contract.
d) The definition of a body of knowledge, from coding through to human management, is a pre-requisite for mapping professional roles against the appropriate professional body.
e) Roles should be categorised to aid understanding for those considering working in cyber security and information risk (i.e. not yet already involved in the profession)
f) Leadership in cyber security should focus on the development of ethics and good practices as lived behaviour in a day-to-day setting.
g) Accreditation should be led by the professional bodies.
h) Professional bodies must instigate processes for addressing and redressing complaints.
i) There may be room to revisit the role of independent and other bodies such as the Information Commissioner in the case of consumer appeals.
j) Contractual mechanisms are starting to be used in procurement to ensure IA good practice. However, it is another matter to hold the company or individual to account when things go wrong. This must also mean the establishment of mechanisms to address and redress fault.
k) Career pathways must allow people to go deeper or across, as well as upwards.
l) Whilst people with hybrid skills (technical and business) are essential (particularly in leadership), it is important that organisations recruit for teams and not just individuals with every skill. This will allow people with well-developed skills in a particular area to fit into a broader team.
m) Public and private sector procurement processes should continue to lead in mandating cyber security standards as part of their procurement. This includes employment of appropriately accredited organisations and professionals.

Introduction and context

Recent years have seen growing concern about the cyber security skills shortage, both in terms of capacity and competence. For those working in the area this is set against a long-running debate about standards, skills, knowledge and professionalism. Consequently, numerous initiatives have been established to attract people into a cyber security career. These include skills frameworks, postgraduate qualifications, internships, summer camps and apprenticeships.

Cyber security is perceived to be a new discipline. In fact, its history can be traced back far beyond the digital age. Codes and cyphers are evident from ancient times; computing can trace its origins to at least the 18th Century, with electronic communications becoming established and taking root for well over 100 years. During this time, professional bodies became well established for the professions of the physical world of engineering, with a focus on buildings and structures and, more recently, electronic systems. The purpose of these bodies was not only to provide a benchmark for those seeking to enter these professions but also to give confidence to the employer or the consumer that the skills they are hiring are *bona fide.* As yet, however, there is no such body for the specific areas of secure software development and the secure handling of information, on which society increasingly depends.

Public, as well as specialist, debate suggests that cyber security needs to be recognised, and accountable, as a specific skills set. Specifically, cyber security is not solely about technical benchmarks but increasingly about ethical, as well as human, behaviours and interactions, all of them dependent on a set of technological interdependencies. These include:

- the incremental development of computing into the complex system of systems of today;
- the development of large scale data bases, introducing a range of privacy and security issues;
- a revolution in online services embodying electronic and computerised controls systems in industry and the home;
- a growth in adoption, first at corporate then increasingly at citizen level;
- the consequent market response, in which many providers have operated on the basis of 'pile it high, sell it cheap, patch it later';
- an environment in which security is therefore perceived to be an overhead, rather than an enabler;
- the establishment, therefore, of an environment which is inherently vulnerable to the interests of criminal or other nefarious actors.

From its first beginnings, the internet was perceived to be a shared space, and this has remained a hallmark of its operation. Sadly, not everyone shares alike, and there has been something of a catch-up game as various malefactors seek to exploit these wider benefits. Cyber security is thereforea relatively new discipline and ensuring the adequate protections, from citizen through corporate to government, an urgent problem.

Numerous workforce surveys show significant skills gaps in the cyber security arena. Skills demand is high, reflected in high pay rates and the rate of churn as people move, or are

poached, from one role to another. Yet demand continues to outstrip supply. In 2013 IAAC ran an internship pilot scheme, with government funding, to identify the perceived gap between the skills delivered by UK education institutions versus employer needs; this, and subsequent research, has identified a number of associated areas blocking those who might otherwise consider cyber security as a career path.

Given the current skills shortage, there is a demand for clear information about cyber security as a career or profession. It has not always been easy to provide it. In part this is because some of the technical language, job titles and concepts make it hard to communicate to a lay audience. In part this has been because the profession, while ostensibly based on the IT sector, spans engineers, psychologists, technologists, lawyers and business leaders. Moreover, citizens – be they private individuals or employees - have their part to play in keeping safe in cyberspace.

Coding and the internet have blurred the lines between software and hardware systems, between user and developer, between professional and hobbyist, between home and abroad. To have a well-designed and managed system requires all to play their part. Communicating clear and consistent information about cyber security is, therefore, complicated by the pace of change and an incoherent narrative about careers and profession.

Research aim and report

Against this background, IAAC ran a research programme to:

Take stock and consolidate views of the cyber security and information risk profession.

This report is the result of four workshops drawing on the expertise of members of the IAAC community, many of whom contributed their personal time, together with IAAC's own desk research. It aspires to create a straight-forward narrative regarding the profession and to appeal to a wide audience, from careers advisers to prospective employees and professional bodies. The report starts by briefly describing the research approach. The themes that emerged are then outlined and discussed before recommendations are made.

Research problem and structure

In the early stages of this research it became clear that there was no generally accepted unifying narrative of a profession. Professionals involved in information assurance and cyber security could be found across many disciplines including engineering, technology, business, social science, compliance and the law. It was clear that talking about cyber security as though it were the medicine or legal profession was not a direct fit, a point explored further below. Yet it remains commonplace for people in the community to talk about cyber security professionals[1] and generally understand that it involves a wide range of

[1] For example, see Sean Martin, 'Cyber security professionals: five ways to increase the talent pool' Tech Target. Available at http://searchsecurity.techtarget.com/feature/Cybersecurity-professionals-

competencies.[2] In an effort to understand this dynamic and logic, it was proposed to examine 'the profession' through four lenses, each of which was explored through a workshop. The aim was to shed light on professionals, professionalism and the profession, such that that the strengths and limitations of 'profession' thinking in information assurance and cyber security could be understood and expressed coherently. The four lenses were:

- **The profession as a community.** Given the range of competencies required, the profession might be understood by examining who is in it and how they relate to one another. This workshop was the first, and was also a scoping workshop for the whole research programme, including the profession concept. This workshop was in part facilitated by established information security professional and author, Andrea Simmons, drawing on her research on professionalization of information assurance.

- **The profession as a set of skills and knowledge**. Based on the findings from the first workshop, it was felt that the profession might be understood by examining the skills and knowledge within its domain. This workshop was supported by the Institute of Information Security Professionals (IISP).

- **The profession as career**. It was also felt that that the structure of work in cyber security and information assurance might shed light on who is recruited, how their career develops and where it takes them. This workshop was conducted in association with the Cyber Security Challenge UK, together with the National Autistic Society, on grounds that consideration of neuro diversity would be helpful in its own right as well as shining light on career structures in general.

- **The profession as a set of ethical behaviours**. Perhaps at the core of professionalism is the way people act and the standards to which they hold themselves. This workshop was facilitated by Professor Philip McCormack, Professor of Practical Ethics at the University of Worcester, and senior army chaplain.

Although designed as separate workshops, it was clear that there were many overlapping themes emerging throughout. Rather than present a chronological record of the workshops, this report presents a thematic summary below.

Themes emerging from the research

Several major themes emerged in this research. The idea of a profession in cyber, and the changing nature of careers, illustrated the contemporary context of the discussion in which a diverse community engages. These themes prompted a discussion of analogy to other professions; regulation and behaviours; questions of ethics, and careers jobs, skills and knowledge. Each of these are explored in turn.

Five-ways-to-increase-the-talent-pool . Accessed 1st February 2017.

[2] For example see Future of Tech, 'The importance of keeping cyber security skills sharp'. Available at: http://www.futureoftech.co.uk/cyber-security/the-importance-of-keeping-cyber-security-skills-sharp. Accessed 1st February 2017.

A profession

The Oxford English Dictionary defines a profession as:

'A paid occupation, especially one that involves prolonged training and a formal qualification'. Middle English… via Old French from Latin… from profiteri 'declare publicly'. [It] derives from the notion of an occupation that one 'professes' to be skilled in.'[3]

Taking this definition, IAAC posed the question: 'what do we declare publicly?' By taking this approach, IAAC aimed to help the profession as a community to describe who are 'we'. This identified three core elements:

a) the notion of a contract, in which someone is paid for work;
b) training - which is caveated with the word 'prolonged';
c) the notion of a formal qualification.

The observation at (b) is particularly informative, as it indicates that an element of experience or longevity is required to gain professional competence in this area. From the perspective of the profession, it is therefore a combination of education, training and skills – the last deriving in part from experience.

Qualifications and training nonetheless remain fragmented and there is no accepted standard around which all can unite. Against the 'profession' definition above, given so much flux and development, it is not unreasonable to ask if an information assurance or cyber security profession exists at all.

The Obligations of a Profession

During IAAC deliberations, our experts also considered the obligations of a profession towards the citizen. Here, we took as our baseline a parliamentary speech from Lord Benson in 1992 in which he set out nine obligations on a profession towards the public it serves:

> *"First, the profession must be controlled by a governing body which in professional matters directs the behaviour of its members. For their part the members have a responsibility to subordinate their selfish private interests in favour of support for the governing body.*
>
> *Secondly, the governing body must set adequate standards of education as a condition of entry and thereafter ensure that students obtain an acceptable standard of professional competence. Training and education do not stop at qualification. They must continue throughout the member's professional life.*
>
> *Thirdly, the governing body must set the ethical rules and professional standards*

[3] Oxford Living Dictionaries. Available at https://en.oxforddictionaries.com/definition/profession . Accessed 1st February 2017

which are to be observed by the members. They should be higher than those established by the general law.

Fourthly, the rules and standards enforced by the governing body should be designed for the benefit of the public and not for the private advantage of the members.

Fifthly, the governing body must take disciplinary action, including, if necessary, expulsion from membership should the rules and standards it lays down not be observed or should a member be guilty of bad professional work.

Sixthly, work is often reserved to a profession by statute — not because it was for the advantage of the members but because, for the protection of the public, it should be carried out only by persons with the requisite training, standards and disciplines.

Seventh, the governing body must satisfy itself that there is fair and open competition in the practice of the profession so that the public are not at risk of being exploited. It follows that members in practice must give information to the public about their experience, competence, capacity to do the work and the fees payable.

Eighth, the members of the profession, whether in practice or in employment, must be independent in thought and outlook. They must be willing to speak their minds without fear or favour. They must not allow themselves to be put under the control or dominance of any person or organisation which could impair that independence.

Ninth, in its specific field of learning a profession must give leadership to the public it serves."[4]

Many at the workshops felt that these obligations are not met by a single professional body, but rather that different parts of the community are accountable to different bodies - and some not at all. Professions such as accountancy, law, medicine have their professional bodies. For medicine, and for 'conventional' engineering, this comprises a network of professional bodies depending on the core skills in which the individual claims to be skilled; given the range of disciplines involved, something similar might be applicable to cyber security.

Consequently, in describing the profession there are two key problems to be addressed. First is the diversity of the different types of people and job role involved in keeping information and systems secure. Second, is the multiple professional bodies that are part of the cyber security landscape.

[4] Lord Benson, *Hansard*, House of Lords Debate, 8 July 1992, Vol 538, cc1198-234. Available at http://hansard.millbanksystems.com/lords/1992/jul/08/the-professions . Accessed on 1st February 2017.

Before returning to these questions in discussion, it is worth examining the community of practice in more detail.

Mapping the community

The Information Assurance Collaboration Group (IACG) and IAAC are currently in the process of reviewing the UK IA Community Map, previously sponsored by CESG and currently in collaboration with the National Cyber Security Centre (NCSC). The previous published version, dating to 2014,[5] lists bodies under the following top-level headings:

- Government
- Professional bodies
- Academic and Research Bodies
- Government/ Industry Groups
- International forums
- Regulatory bodies
- Trade associations and industry groups
- Others

The map clearly shows the wide range of interested parties involved in the security of information and systems, from across industry, education and the public sector, albeit largely by institution. At a more granular level, some of those practitioners will have a clear cyber security role - such as a cyber security analyst responsible for defending a network, or an HR manager responsible for administering recruitment processes and managing insider threat processes. The complexity of this context is compounded when one adds to this systems administrators and engineering disciplines such as software development, which should require developers to think about security when writing code.

One can, therefore, map the community not just by organisation, but by those who have cyber security as a defined prime function and those who have it as an implicit part of their job. Consequently, a matrix or network of responsibilities are carried across multiple roles in any one organisation and by different organisations. Attempting to map the community in this way illustrates how difficult it is to assume that any one body could be the professional body for information assurance or cyber security. This too will be considered later in this report.

Regulation and behaviour change

One analogy repeatedly raised at the workshops was that of the medical profession, given that it encompasses a range of competencies from doctors, anaesthetists, surgeons and nurses through to mid-wives. Each of these has their own professional body and disciplinary processes. This shows that a profession does not have to have just one professional body.

[5] IACG, UK IA Community Map V 5. Available at https://www.ncsc.gov.uk/content/files/protected_files/document_files/uk_ia_community.pdf . Accessed on 1st February 2017.

In their dealings with patients, medical personnel are held to a high level of ethical behaviour and clear lines for complaint and redress are available, even if it is not always easy to establish where blame lies. Similarly, the patient (all of us) must take some responsibility for their own health, as we do for our own information security.

The IAAC research report on Smart Living published in 2016[6] noted that any compliance regime, in this case the discipline of a professional body, should consider several enforcement dimensions such as:

- Risk of being reported
- Risk of inspection
- Risk of detection
- Risk of sanction
- Severity of sanction

Each of these would have to be considered and weighed-up by any professional body and practitioner. What would have to be in place to make these an effective reality in today's cyber security market?

It is not clear the extent to which anyone risks sanction by a professional body for incompetence or unethical behaviour, which indicates some level in immaturity as a profession. Indeed, companies are not always able to question or judge the effectiveness of their hired-in security consultant, nor is harm always obvious, as it might be in the case of a medical mistake or wrong-doing. We also noted in our Smart Living report, that the complexity of a highly-connected system of systems was creating complex liability chains, in which proving blame was becoming more difficult.

Consequently, not only has a culture of holding people to account in cyber security been slow to develop in general, though some sectors have taken it more seriously, but it has also been argued that there is little economic incentive to do so.[7] Many companies want to produce software and components as cheaply as possible, whilst avoiding liability. Nevertheless, economic incentives may be starting to change.

The workshops discussed several ways in which regulation is shaping incentives. Through contracting procedures and recruitment processes, the specific qualifications required for a role or contract are being formalised. For example, 'Since October 2014 Cyber Essentials has been mandatory for suppliers of Government contracts which involve handling personal information and providing some ICT products and services'.[8] 'Cyber Essentials' is a scheme

[6] IAAC, *Security, safety and trustworthiness in smart-living*, 2016. Available at http://www.iaac.org.uk/media/1400/2016-09-22-iaac_smart-living-final.pdf Accessed 19th February 2017.

[7] For example see R Anderson and T Moore, *Information Security Economics – and beyond*. Cambridge University paper available at https://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf Accessed 19th February 2017.

[8] HM Government, 'Protect your business against cyber threats'. Available at: https://www.cyberaware.gov.uk/cyberessentials/ Accessed 19th February 2017.

which helps companies assess their security posture against basic security measures. MOD Suppliers now must answer a question in pre-qualification regarding the cyber essentials scheme.[9] More broadly outside of government, a consensus on which qualifications are required for job roles is still in development.

Forthcoming European Legislation will also change incentives through the threat of the severe punitive consequences regarding data breaches under the General Data Protection Regulation (GDPR). This sits alongside the Network and Information Security Directive (NISD), which places reporting responsibilities on critical national infrastructure, including digital. Both will go live in May 2018.

A question of ethics

There will be many who argue that without a stick or threat of sanction by a professional body, no code of conduct or ethics can be effective. Many bodies produce ethics statements. For example, a short list of ethical principles has been established by the Engineering Council and the Royal Academy of Engineering.[10] At a top level these are:

1. Accuracy and rigour
2. Honesty and integrity
3. Respect for life, law and public good
4. Responsible leadership: listening and informing

The Sans Institute also provides a list of good behaviours that set out what professional and ethical behaviour looks like.[11] At a top level they are:

1. I will strive to know myself and be honest about my capability
2. I will conduct my business in a manner that assures the IT profession is considered one of integrity and professionalism
3. I respect privacy and confidentiality

However, deliberations during the ethics workshop made it clear that, whilst it is good and necessary that codes exist, people do not generally need to memorise them to know what is the right thing to do. With or without the code, when asked most people would see themselves as wishing to act ethically. That they do not is not simply a lack of sanctions for the behaviour, rather it may be the result of several factors.

---

[9] UK MOD, 'MOD Implementation of Cyber Essential Scheme', *Defence Contracts Online*, 2 December 2015. Available at: https://www.contracts.mod.uk/announcements/mod-implementation-of-cyber-essentials-scheme/ Accessed 19th February 2017.

[10] Engineering Council and Royal Academy of Engineering, 'Statement of Ethical Principles for the engineering profession', 2014. Available at: http://www.raeng.org.uk/publications/other/statement-of-ethical-principles Accessed 19th February 2017.

[11] SANS, 'IT Code of Ethics', Version 1,.0 – April 2004. Available at: https://www.sans.org/security-resources/ethics Accessed 19th February 2017.

One theory is related to 'ethical blindness'[12]. This is where, in carrying out tasks, people fail to see their activity as being a matter involving ethics. For example: in manufacturing, an engineering project may be simply seen functionally as the connecting of components and services rather than something involving ethics. Similarly, a software development programme may be seen in financial rather than ethical terms. In other words, during our normal duties we see the task at hand as functional and administrative rather than something with an ethical dimension. It is not that anyone intends to be unethical or do the wrong thing, it is that actions are not seen in ethical terms.

This phenomenon may be because people are remote from the consequences of their actions, or because they remove themselves from the consequences of their actions by subordinating themselves to the authority of those for whom they work. The concept of agency and accountability is notably explored in the work of Stanley Milgram[13] which illustrates that people can ignore ethical considerations if they feel that it is someone else's responsibility to think about it, and theirs is simply to do what is asked of them (Milgram calls this the 'Agentic Sate'). It could be argued that the risk is greater where it appears to relate to a product – in this case, information technology – rather than to people, even though it is people who will be potentially the victims as much as the beneficiaries.

Whilst it is clear that a code of ethics and holding people to account in the end will be a crucial part of any professionalisation approach, it is not the only influence. To avoid ethical blindness and the impact of agentic state, several measures were proposed at the ethics workshop:

a) people have to be encouraged to reflect on their work and encouraged to think about its ethical dimension
b) doing small things well creates good habits that build good character.
c) this only happens if good character, reflection and habits are lived within the social group or organisation.
d) people have to see others around them behaving well, and that that was likely to be the result of **effective leadership.**

Careers, Jobs, Skills and knowledge

The second and third workshops examined skills and careers. The skills workshop started with a presentation from the Institute of Information Security professionals (IISP) supported by material drawn from an internet search, which indicated the skills, knowledge and career paths proposed by a variety of organisations. It was agreed that:

- There a was widening range of roles and criteria for cyber professionals. Consequently:
    - career pathways and associated training are currently ill-defined. For

[12] G. Palazzo, F. Krings, U. Hoffrage, 'Ethical blindness', *Journal of Business Ethics*, February 2013. Available at https://www.researchgate.net/publication/256046104_Ethical_Blindness Accessed 19th February 2017.
[13] S. Milgram, *Obedience to authority: an experimental view*, HarperCollins, 1974.

example, various documents from government and others trying to explain the cyber landscape in the UK often read as a catalogue of diverse initiatives, rather than a narrative of a coherent career or profession; [14]
    - Bodies of knowledge are fragmented, incomplete and inconsistent. It is necessary to define such a body of knowledge in order to establish the various skills, aptitudes and capabilities that the profession might require;
    - Cyber Security needs to encompass disciplines including coding, software development and design, systems engineering and architecture, information management, data processing, psychology, law, education and training.

- With the exception of highly specified skills such as penetration testers (CREST) and other, largely technology-based bodies, there are few formal accredited professional requirements encompassing the gamut of cyber skills;
- There are many 'self-proclaimed' professionals working in the domain;
- There is a high degree of movement into the domain from other professions, including HR and physical or personnel security, even though these would not be recognised as cyber skills.

Cyber security skills are normally differentiated by an ascending level of skill.

The IISP skills framework[15] has been recently reviewed and now includes 6 levels as follows:

1/2: Knowledge
3: Practitioner
4: Experienced Practitioner – basic tasks without supervision, complex tasks with supervision
5: Skilled Practitioner
6: Expert

There are two clear dynamics in this categorisation. The first is the distinction between knowledge and skills. The other is the degree to which a person works under supervision or independently.

The above skills framework has formed the basis for GCHQ accreditation of post graduate degrees and commercial training providers, now being taken forward by the National Cyber Security Centre (NCSC). The content of courses is mapped to cyber security disciplines such as:

[14] For example see K Martin, *Cyber Security Education*, *Qualification and Training*. 2015. Available at https://pure.royalholloway.ac.uk/portal/files/25218802/IETEducationTraining.pdf . Accessed 8th February 2017 and HM Government, Cyber security skills: a guide for business, December 2014. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386248/bis-14-1276-cyber-security-skills-a-guide-for-business.pdf. Accessed 8th February 2017.
[15] IISP Skills framework 2.0. A copy can be requested at https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx Accessed on 8th February 2017

- Information security management
- Information risk management
- Implementing secure systems
- Information assurance methodologies and testing
- Operational security management
- Incident management
- Audit, assurance and review

Competency based skills frameworks indicate developing expertise and skilfulness in these disciplines. As a career path, however, these 'terms of art' remain a potential barrier to those from a non-technical background, even though information security has a significant people, as well as technology, dimension.

Cyber security careers are often represented in an ascending level of seniority - Cyber security jobs have multiple variations on job titles, often difficult to decode.

Whilst one might assume that a developing competency might also mean an increase in seniority, this is not necessarily the case. The comprehensive 'Inspired Careers' website[16], is sponsored by the UK Government, various companies and implemented by the Centre for Research and Evidence on Security Threats (CREST). It allows the visitor to browse cyber security careers and segments a career into the following categories and associate job roles, each of which have explanatory media on the website.

Trainee/Junior	Junior Unqualified Vulnerability Assessor Technical Security Researcher Junior Programmer Security Administrator Systems Administrator (with security) Network Administrator (with security) Risk & Regulatory Trainee	Access Control Administrator NOC Operation Intrusion Analyst SOC Analyst Incident Response Centre Analyst Database Security Administrator Cyber Sales Support Researcher/Lead Generation
Practitioner	Vulnerability Assessor Practitioner Cyber Threat Intelligence Analyst Junior Malware Researcher Cyber Security Forensics Analyst PCI Consultant 27001 Auditor Accreditor Practitioner CCP COMSEC Practitioner CCP Senior SOC Analyst Intrusion Analyst	Cyber Sales Engineer Channel Marketing Manager Professional Services Marketing Manager Product Marketing Manager Product Manager Recruitment Consultant Researcher (Academia) Awareness Programme Facilitator Data Protection Officer Database Security Manager
Senior Practitioner	Penetration Tester (general) Evaluation Facility Product Tester Security Software Developer Security Architect/Senior Architect Senior Security Auditor	Senior Forensics Analyst Cyber Pre-sales Consultant Security Sales Executive Security Business Development Manager

[16] Inspired Careers, Available at http://www.inspiredcareers.org/browse-careers/cyber-security/ Accessed 8th February 2017.

	Compliance Manager Senior Accreditor CCP Senior COMSEC CCP Security Operations Manager Cyber Incident Response Specialist Senior Intrusion Analyst	Technical Account Manager Senior Recruitment Consultant Security Lecturer Security Services Account Manager Awareness Programme Coordinator Cyber Security Specialist Journalist Data Owner
Principal	Specialist Infrastructure Tester Specialist Application Tester Targeted Attack Specialist Malware Reverse Engineer Principal Security Architect Principal Security Auditor Head of Compliance Information Security Manager Lead Accreditor CCP Lead COMSEC CCP Host-based Network Intrusion Analyst	Senior Cyber Security Incident Response Coordinator Network-based Intrusion Analyst Senior Database Administrator Security Product or Professional Services Sales Manager/Director Channel Account Manager/Director Principal Recruitment Consultant Head of Internal Recruitment Senior Lecturer Technical Director
Lead	Partner/Head of Division/CEO Cyber Security Professional Services Chief Information Officer (CIO) Chief Information Security Officer (CISO) Head of Division/CEO Cyber Security Software Product	Professor Head of Division/CEO Cyber Security Hardware Product Chief Technology Officer Industry Influencer Head of Internal Audit/Audit Partner

This site is detailed and indicates the variety of roles in the cyber security profession, particularly its more technological aspects. In terms of the narrative of a profession and its progression, the workshop participants felt that the multiple job roles described made it hard for someone exploring a career to comprehend the profession as a whole, though the overarching concept of 'digital defender' was recognised as partly fulfilling this function on the website.

Cyber security careers are often presented as highly technical

It was felt by workshop attendees that the cyber security profession, despite the widening of the skills involved, exhibited job adverts, industry overviews and training specification for apprenticeships, tended to focus narrowly on the more technical disciplines involved. This list of example jobs below was found on the US NICCS website on 5th July 2016[17] (since updated online – see below):

Chief Information Security Officer (CISO)	Security Architect
Computer Crime Investigator	Security Analyst
Computer Security Incident Responder	Security Consultant
Cryptanalyst	Security Engineer
Cryptographer	Security Operations Center Analyst
Disaster Recovery Analyst	Security Systems Administrator
	Security Software Developer
Forensics Expert	Source Code Auditor

[17] US National Initiative for Cybersecurity Careers and Studies (NICCS), Cybersecurity Careers. Available at https://niccs.us-cert.gov/careers/cybersecurity-careers . Accessed 5th July 2016.

Incident Responder Information Assurance Analyst Intrusion Detection Specialist Network Security Engineer	Virus Technician Vulnerability Assessor Web Penetration Tester

This may reflect the underlying technological nature of cyber security, or where the shortage of skilled people is at its acutest. This can also be seen in initiatives which seek to develop the workforce by identifying people with coding or network knowledge and skills. Yet, while advertised posts appear to place technology skills at a premium, employers are increasingly demanding cyber security experts whose skills encompass interpersonal and communications ability, particularly when working across complex organisations. This, together with the rapid change of technology at operational level, begs the question of which skills sets are required at which point of the cyber skills career pyramid.

It is worth noting that the page with these job roles has since been replaced and clicking on the link takes visitors to NICCS' workforce development page. This now has a link to a 'cyber security workforce framework'[18] which organises cyber security 'specialty areas' into seven categories. This approach may help mitigate some of the issues discussed above relating to multiple and varied job titles. The categories are:

- Analyse
- Collect and operate
- Investigate
- Operate and maintain
- Oversight and development
- Protect and defend
- Securely Provision ((Sic) – probably 'secure provision' is intended)

The categorisation of roles is discussed later and was seen in the workshops as an important aspect of creating a coherent narrative of cyber security. It should be noted, however, that it does not encompass two of the core skills increasingly appearing on job sites for senior cyber security roles, namely: communicate and collaborate.

Issues with the current view of career and skills

The workshops identified several further issues relating to the current picture of careers and skills, outlined below.

A technological focus belies other skills and leadership

The technological focus belies the full breadth of roles and competencies involved in cyber security and information assurance. For example, business knowledge and leadership are underplayed. The workshop attendees felt that the 'hybrid' role was overlooked in job functions and skills development. This role is one where an individual understands both

[18] US NICCS, Cybersecurity workforce framework. Available at: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework . Accessed 8th February 2017.

technical and business requirements relating to the information asset. It was seen as increasingly necessary if organisations were to put information at the heart of their business, and not leave the information asset's strategic exploitation and security solely to a technical team.

The need for careers to facilitate going deeper and not just upwards

Whilst competency is seen in terms of increasing expertise, careers are often seen in terms of progressing in seniority. These can become unhelpfully confused. It was felt in the workshops that not enough attention is being given to those who want to deepen their knowledge in their career rather than become more senior in promotion. For example, considerable time was spent in the third workshop looking at how the profession could accommodate people with enhanced technical skills on the autistic spectrum, and who may not seek a conventional career in terms of promotion and seniority. It is suggested that career pathways should facilitate opportunities to go deeper, and not just upwards. This sits in contrast to the notion of a 'hybrid' professional above and indicates that career pathways need to be flexible to accommodate the personal ambitions and skills of individuals.

Focus on teams and not just individuals

A tendency was perceived where organisations try to recruit people who can demonstrate both technical and softer skills, such as communication and leadership. Consequently, job adverts often wish to recruit the rounded professional, good at everything. However, in championing diversity, it is clear that not everyone, indeed few, may possess that level of roundedness. Consequently, people with highly developed technical skills, but weaker communication skills, may be put off by job adverts demanding competence across skills. Likewise, someone lacking in technical skills, but strong on problem solving may not be given their chance to develop their potential. It was felt at the workshops that this might be mitigated by recruiting for teams which show a rounded set of skills, and not thinking simply about finding them in every individual. This may require some flexibility and alternative means of recruiting and attracting talent.

Think beyond recruitment to whole career pathways

IAAC consultations found that too much attention was being placed on how to get into cyber security and not enough on where it might take someone. In other words, attention was focused on recruitment, but not on the whole story of how someone might move out of cyber security to another area (management, finance or other functions), taking with them transferable skills. Whilst this is understandable at a time of skills shortage, it was felt that a complete picture of a career would need to examine the opportunities it opens in wider business, engineering or other discipline. This might also help attract people into a career in cyber security.

Recognise that a new profession is creating a new culture.

Security tends to have been seen as a speciality to which one comes later in a career, often

building on a background in government, law enforcement or the armed forces. Junior entry into the profession therefore sits against a culture developed by people in their mid and later career, frequently colouring recruitment processes, particularly for the new entrant. This has perhaps made it difficult for today's security professionals to view a whole career as 'cradle-to-grave' and to think of alternative pathways beyond their own experience.

The culture of careers is changing

It was felt that the very notion of a career itself is changing. As people change jobs and roles more frequently there is more inclination to jump between careers and to package knowledge and information in different ways. On the one hand, this can help drive innovation.[19] However, when this is set against the diversity of skills discussed in this paper, the idea of a single overarching professional body that covers all professionals is potentially more problematic when set against an individual's life of different careers or job roles

[19] Spencer Thompson, Is the career dead? *Huffington Post*, 4th August 2013. Available at http://www.huffingtonpost.com/spencer-thompson/is-the-career-dead_b_3384422.html Accessed 8th February 2017.

CONCLUSION AND RECOMMENDATIONS

In this paper, we have explored a number of dynamics of the profession. We have identified the following fundamentals in shaping the narrative of the cyber security profession and professionalism:

1. The diversity of types of people and job role involved in keeping information and systems secure;
2. A consequent multiplicity of professional bodies that are part of the cyber security landscape;
3. The resultant difficulty in defining and enforcing common professional standards;
4. The tentative growth of contractual and regulatory pressure, for example by UK government, for organisation to adopt security standards;
5. Ethical blindness;
6. Confusion in the language and terminology of diverse cyber job roles and categories;
7. Assumptions among recruiters when defining job roles, in particular expectations of existing experience.

Whilst it might be tempting to simply declare that a cyber security and information assurance profession does not exist, other models are worth considering. For example, it might be better to talk about a **profession of professions that work together to manage security and mitigate risk**. This might be usefully known as a meta-profession[20] in which a variety of skills and knowledge are assembled from a range of related professions. This establishes a profession of individuals with a network of core and peripheral skills and knowledge. For example, a lawyer involved in privacy work has their own base profession as a lawyer, but may need to develop knowledge in the domain of another, say in security. These would be the meta-skills or knowledge for the lawyer. Conversely, a security technologist who must understand business practice, has their base profession in technology. They do not need to become a business manager, but rather have some skills and knowledge in that area.

The meta-profession idea may also have the advantage of resonating and being consistent with the virtual and cross-cutting nature of cyber, and the changing or evolving nature of a career examined above. Indeed, it can be argued that this construct can help professional bodies collaborate on those issues that no one body can tackle on its own. Such issues include, for example, interdependence in industrial supply chains, or the relationships between enterprises, governments and nations. However, greater clarity is still required on the simple question of who does what and how can they be held professionally accountable.

[20] As meta-data may be seen as data about data, a meta-profession is a profession of professions. For a small example of one application of this idea in the education space see Raoul A. Arreola, 'Summary of the meta-profession concept' Available at http://www.facultyevaluation.org/meta-profession-project/summary-of-the-meta-profess.html Accessed 4th January 2017. Comments on the use of this term are welcome.

Contractual mechanisms are starting to be used in procurement, such the stipulation that suppliers to government must be compliant with Cyber Essentials and Government. Such measures instantiate the idea of a contract between the service provider and their customer, to a given standard, which is at the heart of a profession. However, it is another matter to hold the company to account when things go wrong, let alone the individuals in a contract with a customer. More work can be done on helping professionals think about ethics, but ultimately, unless the individual professional is mandated by contract to belong to a body, enforcement will be unlikely. This must also mean the establishment of mechanisms to address and redress fault – that which, in other professions, would be recognised as being 'struck off'.

On the basis of these discussions and research, IAAC presents the following conclusions:

- It is unlikely that there can be a single professional body for everyone professionally involved in cyber security.
- The cyber security profession should be thought of as a 'meta-profession'.
- The definition of a body of knowledge and skills, from coding through to human management, is a pre-requisite for mapping professional roles against the appropriate professional body.
- Professional bodies and standards must be mandated and mechanisms for addressing and redressing fault established.
- There may be room to revisit the role of independent and other bodies such as the Information Commissioner in the case of consumer appeals.

We set out in Annex A below a possible outline narrative for the Profession and the shape that it might take, in terms of a career path that will likely entail a range of facets. This variety has informed IAAC's key recommendations, which are articulated below.

Recommendations

Whatever the eventual shape of the Profession, a clear narrative can be developed from the deliberations outlined in this report. On the basis of these consultations and research, IAAC offers the following recommendations:

a) Professional bodies and any new initiatives under consideration should review the principles of a profession, set out by Lord Benson in his 1992 speech (see below)
b) It is unlikely that there can be a single professional body for everyone professionally involved in cyber security. It might be better to talk about a **profession of professions that work together to manage security and mitigate risk (**i.e. a 'meta-profession').
c) As a meta-profession, the core skills of the professional would indicate their base professional association, though they may need to belong to more than one body depending on the role they are fulfilling in a contract.
d) The definition of a body of knowledge, from coding through to human management, is a pre-requisite for mapping professional roles against the appropriate professional body.

e) Roles should be categorised to aid understanding for those considering working in cyber security (i.e. not yet already involved in the profession).
f) Leadership in cyber security should focus on the development of ethics and good practices as lived behaviour in a day-to-day setting.
g) Accreditation should be led by the professional bodies.
h) Professional bodies must instigate processes for addressing and redressing complaints.
i) There may be room to revisit the role of independent and other bodies such as the Information Commissioner in the case of consumer appeals.
j) Contractual mechanisms are starting to be used in procurement to ensure IA good practice. However, it is another matter to hold the company or individual to account when things go wrong. This must also mean the establishment of mechanisms to address and redress fault.
k) Career pathways must allow people to go deeper or across, as well as upwards.
l) Whilst people with hybrid skills (technical and business) are essential (particularly in leadership), it is important that organisations recruit for teams and not just individuals with every skill. This will allow people with well-developed skills in a particular area to fit into a broader team.
m) Public and private sector procurement processes should continue to lead in mandating cyber security standards as part of their procurement. This includes employment of appropriately accredited organisations and professionals.

ANNEX A – the Profession: an outline

Below is a 'straw-man' narrative of a cyber security meta-profession, taking into account the discussions outlined in the above paper. Where possible, we indicate job roles against appropriate professional bodies.

GRADE A profession

Jobs in cyber security or information appear under a plethora of titles. Some of the complexity can be better understood by grouping roles into generic headings. To do this we suggest a mnemonic – 'GRADE A'. The roles may be separate or combined in any given organisation.

G	Governors
R	Risk Managers
A	Auditors/ Assessors
D	Defenders (incorporating testers, analysis and operators)
E	Engineers
	&
A	Architects

Governors own or have responsibility or accountability for information, data or security within an organisation. They are usually experienced and senior. For example, a Senior Information Risk Owner (SIRO) in the Public Sector may have the following duties:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs
- Understanding and managing risks inherent in external contractual dependencies
- Advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls
- Owning the organisation's information incident management framework

This role may have responsibility for ensuring that the organisation is compliant with regulations relating to the law (such as data protection) or their sector (such as finance sector specific regulations). This role may also have a key part to play in supporting efforts across the company in getting security right. For example, in supporting HR in its recruitment polices regarding security and setting the right culture and processes. Governors will take account of legal and regulatory matters affecting the business, working with properly qualified legal and security personnel and team members as required.

Risk Managers have a more hands on role relating to assessing and managing information risk or security risk. They will make recommendations based on their assessment on how risks can be managed and mitigated. They will be a person with governance responsibilities. Typical objectives for a cyber risk management role are:

- Establish information risk steering committees
- Create and execute information risk assessments
- Perform / conduct Business Impact Assessments, Threat Profiling and Vulnerability Assessments.

Risk managers will need to have a good understanding of the wider business they support so that they can judge how critical an information asset or system is to the business, should it be attacked or fail. Personnel risk will have a strong HR component or lead.

Auditors/ Assessors. As part of the overall governance process in an organisation, an audit may be conducted to provide a more independent view of the security management within the organisation. This might examine management processes as well as a more technical audit of security. Auditors of a large organisation may assess it against an international standard such as the ISO27001 Information Security Risk Management standard. Increasingly, many smaller organisation (and some larger) are adopting a standard called Cyber Essentials. The enhanced version of this known as Cyber Essential Plus includes an audit by someone from outside the company. Technical assessment may include a penetration test also known as vulnerability assessment. Sometimes techniques used in this are known as ethical hacking techniques.

Typical job objectives include:

- Conduct an ISO 27001 Audit.
- Provide penetration testing services to clients.
- Conduct penetration testing on applications and network.
- Configure and use standard industry tools.

Defenders are the often seen as the frontline of security staff and will conduct a range of Testing, Analysis and Operational (TAO) work. They may be asked to conduct auditing and assessment work depending on their specific role. Typical jobs include working in a Secure Operations Centre (SOC) monitoring a live network and responding to incidents or analysing malware captured on the network. Typical job objectives for SOC analysts' work include:

- Identify current and future threat and recommend remedial actions.
- Work as part of a 24/7/365 team delivering real time proactive monitoring and maintenance of supported security tools and associated rules and signatures.
- Carry out Triage on Security events, raise incidents and support the Incident Management process
- Ensure that 'lessons identified' are followed through with appropriate changes in processes, training and behaviour
- Create and maintain SIEM (Security Information and Event Management) correlation rules.

Engineers are required to engineer components, systems and processes to provide the services needed, whilst maintaining security. In a general sense, all engineers should ensure that what they produce is secure by design and by default. For example, a software

engineer should avoid accidentally introducing security vulnerabilities into their software when they are writing it. In a specific sense, some of the roles above may have an engineer title, such as SOC engineer. It too might have the job objective listed above but also engineering tasks such as:

- Provide engineering analysis, design and support for firewalls, routers, networks and operating systems.
- Develop technical and programmatic assessments, evaluate engineering and integration initiatives and provide technical support to assess security policies, standards and guidelines.
- Review and recommend the installation, modification or replacement of hardware or software components and any configuration change(s) that affects security.

Architects are more like designers than engineers though in practice there may be a large overlap between these roles. Invariably they are interested in the system as a whole. Typical job objectives for a security architect are as follows:

- Identify information risks that arise from proposed IT architectural designs.
- Propose architectural designs and countermeasures that mitigate risk and align with business policy.
- Balance the cost of design countermeasures in line with information risk.
- Ensure the secure configuration of systems in line with design requirements.
- Work closely with solution architects and wider design teams to ensure that accreditation aspects are implemented appropriately.
- Ensure architectural design meets security policy and is an enabler of accreditation.
- Provide and manage an approach to the management of design requirement to support accreditation for legacy systems.

Relevant professional bodies and membership organisations

Given the roles described above there are many organisations that one could join. It is not the purpose of this report to make a recommendation concerning one organisation against another. Indeed, anyone in a role described above would most likely find a home in any of the bodies listed below. However, each has its own culture and focus. For example, some are more focused on professional engineers and security as a part of their broader interest. Others have a specific interest in security, and some on specific aspects of security.

They are highlighted here in no particular order, nor do we claim that this list is exhaustive.

Institution of Engineering and Technology (IET). Tracing its history through amalgamation to 1871, this body is a chartered institute with the mission to 'inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society.' It has a deep interest in security and someone joining it will benefit from an integrated view of an extensive network across the broader engineering community in 150 countries.

Institute of Information Security Professionals (IISP). The institute focuses on people working specifically in an Information Security role. One of its key activities has been the development of the IISP Skills framework which has been adopted by GCHQ and others as a way of accrediting courses by universities and other training providers.

British Computer Society (BCS). The British Computer Society is the chartered institute for IT. Like the IET, it can award chartered engineer status and provides a range of other professional qualifications. It focuses on IT and has a large security interest group integrated with its broader IT perspective. It aims to 'champion the global IT profession and the interests of individuals, engaged in that profession, for the benefit of all'.

CREST. CREST is widely regarded as the standard in penetration testing qualifications. It aims to provide 'organisations wishing to buy penetration testing services with confidence that the work will be carried out by qualified individuals with up to date knowledge, skill and competence of the latest vulnerabilities and techniques used by real attackers.'

$(ISC)^2$. '$(ISC)^2$ is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the Certified Information Systems Security Professional (CISSP) certification it helps shape standards in cyber security by producing guidance and a framework for continuing professional development. CISSP is still widely internationally cited as a qualification for roles such as Chief Information Security Officer. It offers a range of security related qualifications.

ISACA – 'As an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.' ISACA qualifications are well-regarded in the international marketplace. It offers CISM and CISA.

Information Systems Security Association (ISSA). 'ISSA is a nonprofit organization for the information security profession committed to promoting effective cyber security on a global basis.'

ASIS International – 'ASIS International is a global community of security practitioners, each of whom has a role in the protection of assets - people, property, and/or information.'

Other professional bodies are taking an interest in security, but are not security specific, IT or Engineering bodies. For example, the Institute of Personnel and Development lead on human resource issues. The legal profession has its own professional bodies too.

IAAC is not mentioned in the list above as it is not strictly a professionally body. Rather it is a not-for-profit network, sponsored by industry, that brings together a community of some 600 professionals. This includes corporate leaders, government officials, members of the defence, security and law enforcement communities, academics, scientists and technical experts, in order to address the information assurance and related challenges faced by the 'Information Society'. IAAC was founded in 1999. Since then it has been at the leading edge of many of the developments in Information Assurance and Cyber Security thinking in UK,

maintaining a non-partisan position on matters affecting the way society uses and protects information.

As well as the qualification mentioned above in the section on professionals bodies and membership organisations, the UK has seen several initiatives worth mentioning such as:[21]

- GCHQ and the National Cyber Security Centre have a system for accrediting individuals as certified practitioners, based on the IISP skills framework. This has been regarded as necessary for taking government related work though they aspire for this to be seen as a broader industry standard. They have also started to certify courses run by commercial training providers against standards.

- The Tech Partnership have been at the forefront of establishing cyber apprenticeships and degree apprenticeships. For those who wish to go straight into work to earn and learn.

- Universities are now offering specialist postgraduate qualification in cyber, and a few at undergraduate level, where the trend to date has been to develop modules as part of a more general educational programme.

Trying to map specific roles against institutions is challenging, and highly political, not least because IAAC wishes to continue to work with the community at large. Nevertheless, some general conclusions can be reached which may help people identify their institutional home:

- All institutions have an interest and a stake in developing professional standards in security.
- Anyone could conceivably join more than one institution.
- Those who are more engineering, design and architecture orientated, perhaps mixing security with broader engineering practice, should definitely consider joining one of the engineering professional bodies.
- Those with a specific cyber security role should consider a specific institution such as IISP and/ or CREST for the professional development and networking.

Qualifications for specific roles, including in an international context, requires more industry and government consensus. This will most likely follow when business starts to contract for organisations and people with accredited skills and professional standing.

[21] More detail can be found at K Martin, *Cyber Security Education*, *Qualification and Training*. 2015. Available at https://pure.royalholloway.ac.uk/portal/files/25218802/IETEducationTraining.pdf. Accessed 8th February 2017 and HM Government, Cyber security skills: a guide for business, December 2014. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386248/bis-14-1276-cyber-security-skills-a-guide-for-business.pdf. Accessed 8th February 2017.

Report Author: Nigel Jones, CEO IAAC and Louisa-Jayne O'Neill, Vice-Cahir IAAC

IAAC Contact:

Information Assurance Advisory Council
1st Floor Block D, North Star House
North Star Avenue
Swindon, Wiltshire
SN2 1FA United Kingdom
Telephone: +44 (01793) 417453
Email: info@iaac.org.uk

Acknowledgements

IAAC would like to thank the following for their support to this research

Andrea Simmons, http://i3grc.co.uk/about
Peter Fischer, Institute of Information Security Professionals, https://www.iisp.org/imis15
Emma Jones and Richie Maybank, National Autistic Society, http://www.autism.org.uk/
Stephanie Aldridge, Cyber Security Challenge UK, https://cybersecuritychallenge.org.uk/
Professor Philip McCormack, http://www.worcester.ac.uk/

Thanks must also go to the many members of the IAAC Community of Interest who contributed in the research workshops.

In particular, IAAC is grateful to its sponsors.