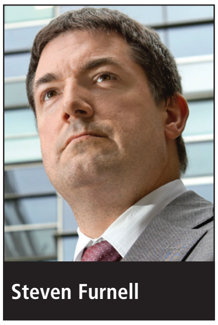
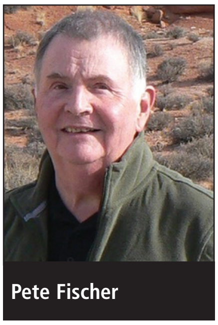
Can't get the staff? The growing need for cyber-security skills


Steven Furnell


Pete Fischer

Amanda Finch

Steven Furnell, Pete Fischer and Amanda Finch, Institute of Information Security Professionals

When we consider the specialist expertise required in the IT sector, cyber-security is definitely an area in which we should want work to be entrusted to suitably skilled professionals. However, while this is easy to say, it raises immediate questions of what it actually means in practice.

The Oxford English Dictionary defines professionalism as: "The ability or skill that you expect from a professional person," while the Merriam-Webster definition refers to "the skill, good judgement, and polite behaviour that is expected from a person who is trained to do a job well." These are clearly characteristics that we would like to see from anyone offering their services to address security issues. However, information security is still a relatively new profession (and its branding as cyber-security is even more recent), which means there is still some debate about the level of professionalism within it. Moreover, organisations that realise they ought to be looking for suitable professionals may not know how to recognise the skills they need and may have trouble finding them.

Hot topic

Considering the latter part of this challenge first, the cyber-security skills shortage has certainly become a hot topic in the wider IT industry. If we look for some supporting evidence then we quickly find that there is no shortage of that, with several sources pointing towards very similar conclusions:

- Back in 2013, the UK's National Audit Office suggested that it could take up to 20 years to bridge the cyber-skills gap.[1]
- A 2015 study from Frost and Sullivan and (ISC)[2] concluded that there will be a global shortfall of around 1.5 million security practitioners by 2020.[2]
- A 2016 study by Foote Partners predicted that while global demand for cyber-security talent will rise to six million by 2019, there will be a shortfall of 1.5 million professionals to fill the positions.[3]
- Cyber Security Ventures reported one million open cyber-security job vacancies in 2016, and projected this would reach 1.5 million by 2019.[4]
- A global study published by Intel Security and the Centre for Strategic and International Studies (CSIS) reported that 82% of respondents considered there to be a shortage of cyber-security skills, with 71% suggesting that direct and measurable damage to organisations occurred as a consequence.[5] Moreover, it was estimated that 15% of the cyber-security positions would remain unfilled by 2020.
- Kaspersky Lab findings from 2016 (based on surveying representatives from over 4,000 companies across different industries and of various sizes) suggested that 50% had observed a growth in wages due to a shortage of talent, 48% experienced a shortage of security talent and 46% felt they needed more security specialists. The study additionally suggested that enterprises lacking security skills can end up spending at least three times as much to recover from security breaches.[6]

Outstripping supply

While the various findings clearly vary in their estimates of the specifics, there is clear agreement that the current and future demand for cyber-security skills looks likely to be outstripping supply. As a result, the recently renewed UK National Cyber Security Strategy identified the need to strengthen cyber-security skills as a key issue.[7] Specifically, it cites the need to tackle the following systemic issues currently contributing to the cyberskills shortage:

- The lack of young people entering the profession.
- The shortage of current cyber-security specialists.

- Insufficient exposure to cyber- and information security concepts in computing courses.
- A shortage of suitably qualified teachers.
- The absence of established career and training pathways into the profession.

As an indication of the impact arising from this, a 2016 report from Databarracks suggested that almost half of UK organisations feel they lack in-house skills to handle the cyberthreats they are facing.[8] It is also relevant to observe that the lack of skills can be a challenge even for the security industry itself: the aforementioned Kaspersky Lab study indicates that the company itself typically needs to interview 40 people in order to hire one expert.

> ***"Given that the skills are in short supply, it is even more important that organisations can correctly judge the ones that they need"***

The overall situation is clearly far from ideal and it is further complicated by varying notions of what being a security professional actually means. Given that the skills are in short supply, it is even more important that organisations can correctly judge the ones that they need. But what should they be looking for? Does it just mean having a relevant degree or holding a professional certification, or should there be some more specific measure of the knowledge and skills involved? In short, where should the skills be expected to come from? To explore these questions, this discussion examines the role of academic qualifications and professional certifications, before moving on to consider a means of bringing clarity to the currently confused picture.

Qualified to help?

On the academic side, there has been a definite growth in the number and range of programmes offering security content, with many now offering it as a named degree title. These can be found at both Bachelors and Masters levels, but the mere presence of cyber-security in the title does not mean the underlying coverage will be the same, and so it is useful to have some means of interpreting the landscape. As an example, in the UK the GCHQ academic certification scheme (which the lead author helped to develop) currently recognises eight degree types, spanning Bachelor's, Integrated Master's and Master's programmes, with coverage ranging from general cyber-security to specific areas of digital forensics and network security.[9] There is also recognition that cyber-security does not exist in isolation, with several of the certified routes requiring a tangible segment of underpinning computer science to accompany it. With this in mind, the specific list of certifications offered at the time of writing are as listed in Table 1.

A growing number of UK academic degrees are certified against these specifications, but there are still a great many that are not and the popularity of the cyber-security domain is leading to more programmes emerging as a result.

At the academic level, appropriate qualification does not necessarily equate to having studied a named security degree (although this can clearly have advantages), but equally it means more than just having a module or two that mention security across the overall programme. What certainly is desirable is for coverage of security to be appropriately embedded in the delivery of other key topics (eg, software engineering, networking, databases, etc), such that it is seen as implicitly relevant to these rather than as a distinct topic to be covered (and attended to) separately.

While academic programmes clearly have the potential to develop new talent and foster the skills that are in demand, it is also important to realise that there will be limits to how far even a Master's level degree will be able to take them. Indeed, the aforementioned Intel/CSIS report also indicated that less than a quarter of respondents felt that education programmes were adequately preparing students to enter the industry.

With this in mind, it is relevant to repeat a quote from the lead author that was published in the aforementioned Kaspersky Lab report: "Care needs to be taken about how much we regard graduates as being directly 'qualified to work' in the IT security field. Even as degree graduates, I would not necessarily regard them as qualified practitioners. They should certainly have a good level of supporting knowledge and some of the skills, but there will equally be various aspects that they have not been able to put into practice 'for real' at that stage". As such, employers should still be prepared to invest in relevant training and allow experience to be gained. Additionally, it may also be relevant to look for other indications of relevant experience.

Certified for cyber?

Looking beyond academic qualifications, the other significant category of 'badge' that security practitioners may hold to signify their skills are professional certifications. Looking at the situation

Level	Degree type
Bachelor's:	Computer Science for Cyber Security
	Computer Science and Cyber Security
Integrated Master's	Computer Science for Cyber Security
	Computer Science and Cyber Security
Master's	General Cyber Security
	Digital Forensics
	Computer Science for Cyber Security
	Computer Network and Internet Security

Table 1: GCHQ certifications for academic degrees.

Certification	Security+	Certified Ethical Hacker (CEH)	GIAC Security Essentials (GSEC)	Certified Information Security Manager (CISM)	Certified Information Systems Security Professional (CISSP)
Provider	CompTIA	EC-Council	SANS	ISACA	(ISC)^2
Role/aim	"Covers the essential principles for network security and risk management – making it an important stepping stone of an IT security career"[12]	"Provides the advanced hacking tools and techniques used by hackers and information security professionals alike to break into an organisation"[13]	"Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts"[14]	"Promotes international security practices and recognises the individual who manages, designs and oversees and assesses an enterprise's information security"[15]	"For those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organisations from growing sophisticated attacks"[16]
Target group	Recommended CompTIA Network+ and two years of experience in IT administration with a security focus	Aimed at security officers, auditors, security professionals, site administrators	Aimed at security professionals who want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks	Aimed at information security managers, aspiring information security managers, IS/IT consultants	Aimed at CISOs, security analysts, security consultants, network architects
Examination	Examined via 90min exam based upon multiple choice and performance-based questions	Examined via 4-hour multiple choice test, with 125 questions	Involves a proctored exam of 180 questions in up to 5 hours	Examined via 4-hour exam, with 200 multiple choice question. Verified evidence of five years of information security work experience, with at least three years information security management experience	Examined via 6-hour exam, with 250 multiple choice, drag & drop and hotspot questions. Candidates must have a minimum of five years cumulative paid full-time work experience in two or more of the eight domains of the CISSP Common Body of Knowledge

Table 2: Overview of leading professional certifications in information security.

here, the landscape is even more varied, with a range of providers – including CompTIA, EC-Council, ISACA, (ISC)^2 and SANS to name but a few – each of which tends to offer a range of related certifications suiting different security specialisations and levels of experience.

As illustrated by a 2015 study from Tittel, Lemons and Kyle, this can lead to a potentially bewildering array of offerings to choose from, with their assessment identifying 57 vendor-neutral general certifications, 24 related to forensics/anti-hacking, and a further eight classified as specialised.[10] To give some further insight into this market, Table 2 summarises a series of certifications identified as the top five leaders in the field for 2016.[11] Each is presented with a brief description of its intended role (quoted directly from the provider's marketing materials), alongside an indication of the target audience and examination (and, where appropriate, experience) requirements. As can be seen from the table, while these five may be similar in terms of all being popular in the market, they are far from the same when it comes to their underlying characteristics.

So, do we know how to recognise the skills we want? Looking at related job adverts one can quickly get the impression that organisations are less than clear on it. For example, consider the following direct quote from a vacancy for an £80,000 role as a cyber-security product manager: "Cyber-security experience or certification preferred, ie, Security+, CISSP, CISA or similar". As can be seen from Table 2, Security+ and CISSP are notably dissimilar in terms of their depth and experience requirements, while the CISA (Certified Information Systems Auditor) certification – offered by ISACA – is another distinct variation again. While all would deliver someone that could be broadly described as holding a security certification, they would come with an assurance of significantly different underlying skills and experience. As such, the approach in the advert feels somewhat analogous to asking for fruit and specifying a preference for an orange, a banana or a pineapple – or similar!

A framework for clarity

The breadth of qualifications and certifications available, combined with the potential confusion when trying to differentiate between them, highlights the need for a means to go beyond the names and acronyms and look at the underlying nature of the skills that exist in the cyber-security domain.

- One means of providing such clarification is the Skills Framework produced by the Institute of Information Security Professionals (IISP). This

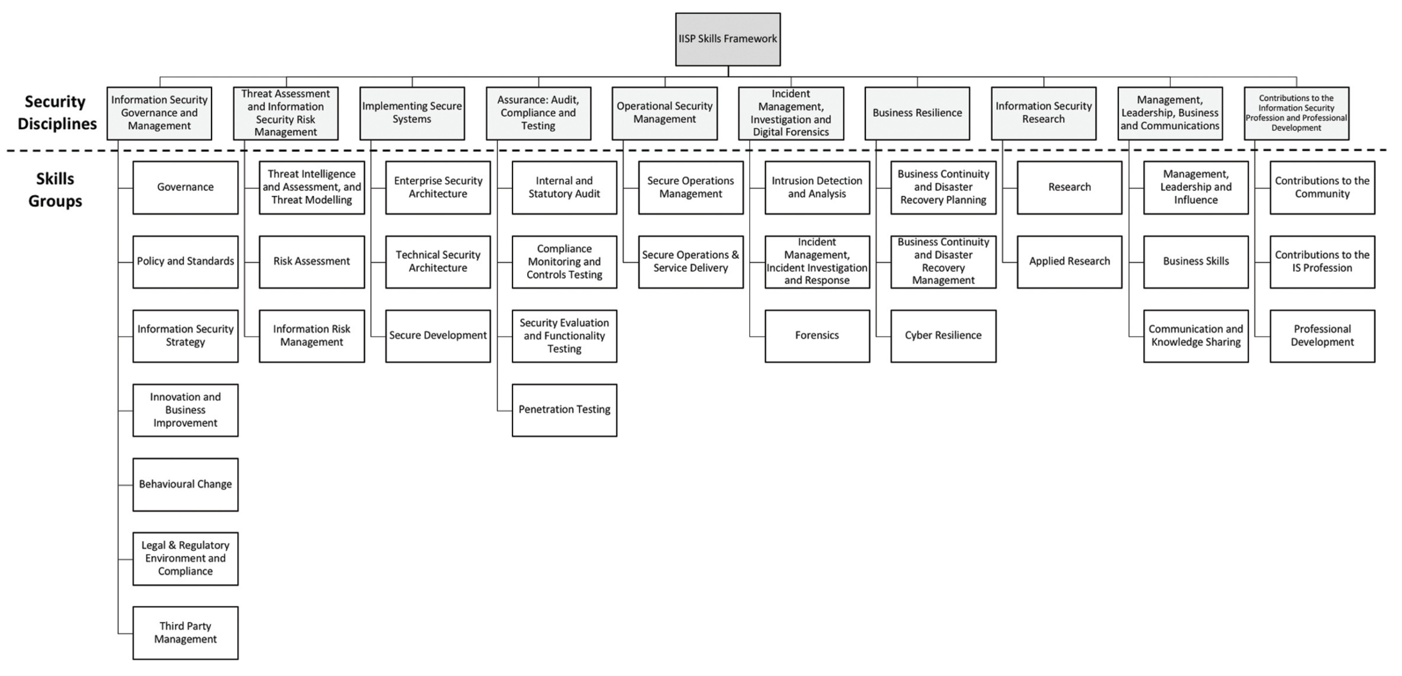

IISP Skills Framework
Security Disciplines
Information Security Governance and Management
Threat Assessment and Information Security Risk Management
Implementing Secure Systems
Assurance: Audit, Compliance and Testing
Operational Security Management
Incident Management, Investigation and Digital Forensics
Business Resilience
Information Security Research
Management, Leadership, Business and Communications
Contributions to the Information Security Profession and Professional Development
Skills Groups
Governance
Policy and Standards
Information Security Strategy
Innovation and Business Improvement
Behavioural Change
Legal & Regulatory Environment and Compliance
Third Party Management
Threat Intelligence and Assessment, and Threat Modelling
Risk Assessment
Information Risk Management
Enterprise Security Architecture
Technical Security Architecture
Secure Development
Internal and Statutory Audit
Compliance Monitoring and Controls Testing
Security Evaluation and Functionality Testing
Penetration Testing
Secure Operations Management
Secure Operations & Service Delivery
Intrusion Detection and Analysis
Incident Management, Incident Investigation and Response
Forensics
Business Continuity and Disaster Recovery Planning
Business Continuity and Disaster Recovery Management
Cyber Resilience
Research
Applied Research
Management, Leadership and Influence
Business Skills
Communication and Knowledge Sharing
Contributions to the Community
Contributions to the IS Profession
Professional Development

Figure 1: The IISP Skills Framework.

was originally established in 2007 and aims to provide the *de facto* standard for measuring competency of information security professionals. To quote from the Framework itself, it provides a means to:[17]

- Describe the range of competencies expected of information security professionals in the effective performance of their roles.
- Define the skills and capability expected of security professionals in practical application and not just an assessment of their knowledge.

The content was developed in collaboration with industry, government and academia and covers the breadth of the infosec/cyber profession. The Framework was refreshed in 2016 and Figure 1 depicts the structure of the latest version, which is organised as 10 security disciplines, each of which then has a set of underlying skills groups.

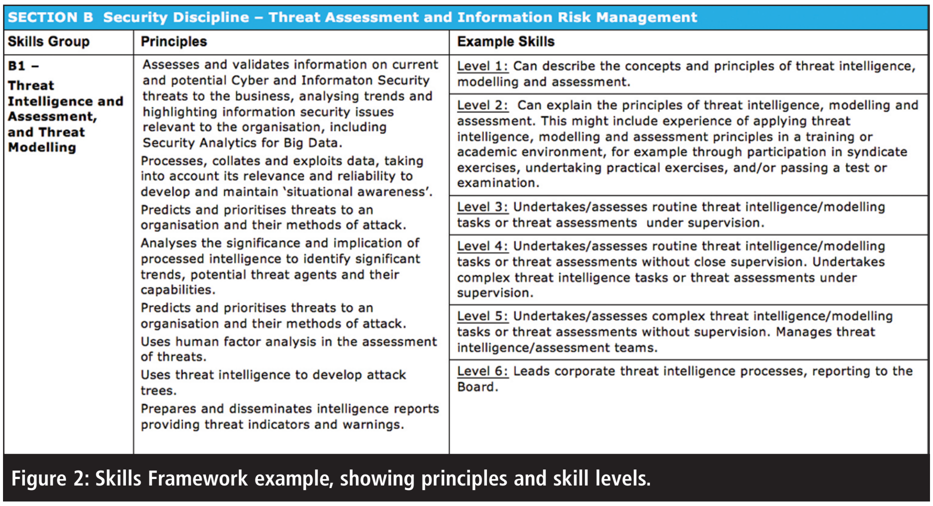
Looking at this breakdown, it is very notable that the skills of interest are not restricted to the security-specific topics and the disciplines denoted towards the right of the diagram are linked to business skills and professionalism. This recognises that rounded security practitioners will often require more than just knowledge and expertise in the security-related topics and that successfully taking this into the organisation requires a number of other skills to support and enable the process. It is also recognised that not all roles require detailed experience in all competency areas.

Recognising that skills exist at different levels, the Framework describes each of the groups at six different levels, ranging from possessing basic knowledge to the ability to lead. These levels are summarised below, noting that the full descriptions also make explicit distinction between the knowledge and practice-related expectations at each level:

- **Level 1 – Knowledge**: basic knowledge of principles/follow good user practice. Has acquired and can demonstrate basic knowledge associated with the skill – eg, through training or self-tuition.
- **Level 2 – Knowledge and Understanding**: knowledge and understanding of basic principles. Understands the skill and its application.
- **Level 3 – Apply**: practitioner – understands the skill and applies it to basic tasks with some supervision.
- **Level 4 – Enable**: senior practitioner – understands the skill and applies it to basic tasks with minimal supervision and to complex tasks with some supervision. Normally operates as a member of a team in a project/programme or system environment.
- **Level 5 – Advise**: principal practitioner – understands the skill and applies it to complex tasks with no supervision. Leads teams in a project/programme or system environment. Operates at a corporate level.
- **Level 6 – Initiate**, Enable, Ensure: expert/lead practitioner – an authority who leads implementation of the skill. Is an acknowledged expert by peers in the skill.

To show an example of how this works in practice, Figure 2 presents an extract from the Skills Framework itself, focusing upon the skills group relating to 'threat intelligence and assessment and threat modelling' and showing how the skills to be expected would vary across the six levels.

The Skills Framework provides a means to map the landscape and understand where the various qualifications and certifications fit in. For the individual, it offers a means of understanding their own skill base, rating their familiarity and experience of the different groups against the six skill levels that can be involved (from basic following of good practice to operating as a lead practitioner).



SECTION B Security Discipline – Threat Assessment and Information Risk Management		
Skills Group	**Principles**	**Example Skills**
B1 – **Threat Intelligence and Assessment, and Threat Modelling**	Assesses and validates information on current and potential Cyber and Informaton Security threats to the business, analysing trends and highlighting information security issues relevant to the organisation, including Security Analytics for Big Data. Processes, collates and exploits data, taking into account its relevance and reliability to develop and maintain 'situational awareness'. Predicts and prioritises threats to an organisation and their methods of attack. Analyses the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities. Predicts and prioritises threats to an organisation and their methods of attack. Uses human factor analysis in the assessment of threats. Uses threat intelligence to develop attack trees. Prepares and disseminates intelligence reports providing threat indicators and warnings.	Level 1: Can describe the concepts and principles of threat intelligence, modelling and assessment. Level 2: Can explain the principles of threat intelligence, modelling and assessment. This might include experience of applying threat intelligence, modelling and assessment principles in a training or academic environment, for example through participation in syndicate exercises, undertaking practical exercises, and/or passing a test or examination. Level 3: Undertakes/assesses routine threat intelligence/modelling tasks or threat assessments under supervision. Level 4: Undertakes/assesses routine threat intelligence/modelling tasks or threat assessments without close supervision. Undertakes complex threat intelligence tasks or threat assessments under supervision. Level 5: Undertakes/assesses complex threat intelligence/modelling tasks or threat assessments without supervision. Manages threat intelligence/assessment teams. Level 6: Leads corporate threat intelligence processes, reporting to the Board.

Figure 2: Skills Framework example, showing principles and skill levels.

The same principle can be used by organisations in recruitment and capability building contexts, to understand the skills they possess and those that they need. Meanwhile, for academic programmes, professional certifications and training courses, a mapping of their content against the Skills Framework will give a clear idea of what is to be expected at the end and thereby aid organisations to better understand the options most suited to their needs. The Skills Framework is already used across government, commerce and education and the ambition is for it to become a common reference for the community as a whole.

Conclusions

Unlike some other aspects of IT, security simply will not work if done badly. You can write bad software that will still run and fulfil its function, but bad security will fail to provide the protection expected. As such, entrusting the tasks to appropriately skilled professionals is a good starting point.

"There are talented people within the workplace, often working within our organisations, that have skills that we need within the profession and the ability to be upskilled to become rounded cyber-security professionals"

However, those seeking qualified professionals need to know what to look for, and an understanding of related certifications and qualifications is necessary if organisations are to make the right choices. It is not a question of some qualifications or certifications being better than others, but it is important to recognise that they are different and understand what they can be expected to provide as a consequence. The IISP Skills Framework is a good reference point in this context, as it provides a means for skills requirements to be expressed in an independent manner and then mapped to the available offerings in the market. Of course, this requires that qualifications, certifications and training programmes are all suitably mapped to the Framework and that organisations have a similar mapping for the role(s) that they need to fill, but with these aspects addressed it provides a means for needs to be matched on a skills-focused basis.

If we are to address the skills shortage, we need to cast our net widely and encourage people to join the profession from a wide range of backgrounds and to trawl within our current workforce. There are talented people within the workplace, often working within our organisations, that have skills that we need within the profession and the ability to be upskilled to become rounded cyber-security professionals. They can bring a strong understanding of business requirements or badly needed technical skills that they are applying in a different environment plus bring experience from their own career journeys. We need to invest in them to help them to upskill appropriately, tailoring development accordingly and if we do that then we can 'fast track' them into becoming security professionals and ensure they have the appropriate qualifications and certifications.

About the authors

Steven Furnell is a professor of information systems security and leads the Centre for Security, Communications & Network Research at Plymouth University. He is also an Adjunct Professor with Edith Cowan University in Western Australia and an Honorary Professor with Nelson Mandela Metropolitan University in South Africa. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 270 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society *(2001) and* Computer Insecurity: Risking the System *(2005). Furnell is the current Chair of Technical Committee 11 (security and privacy) within the International Federation for Information Processing and a member of related working groups on security management, security education and human aspects of security. He is also a board member of the Institute of Information Security Professionals and chairs the academic partnership committee and southwest branch.*

Pete Fischer has over 30 years' experience in information security. He is a Fellow of the Institute of Information Security Professionals (IISP) and chairs its Training Accreditation Committee. In recent years, he has led the review of the IISP Skills Framework which resulted in the publication of Issue 2.0, following which he oversaw a pilot implementation, the feedback from which will be incorporated in Issue 2.1. He is currently supporting work on the development of a Cyber Security Body of Knowledge and chairs the Stakeholder Group which is supporting CESG in its CySec-BOK project. His previous roles include: lecturer in IA *at the National School of Government; head of the Information Assurance and Certification Schemes at CESG; head of the UK Common Criteria Certification Body; and head of Information Security and Accreditation at GCHQ.*

Amanda Finch has specialised in information security management since 1991. In addition to her role as general manager of the IISP she works with the Information Security Forum (ISF) and the British Computer Society (BCS) to gain recognition for the discipline as a recognised profession. She has a Master's degree in Information Security, is a Full and Founder Member of the IISP and a Fellow of the BCS. In 2007 she was awarded European Chief Information Security Officer of the year by Secure Computing *magazine.*

References

1. 'The UK cyber-security strategy: Landscape review'. National Audit Office, 12 Feb 2013. Accessed Dec 2016. www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/.
2. 'The 2015 (ISC)2 Global Information Security Workforce Study'. Frost & Sullivan, Apr 2015. Accessed Dec 2016.
3. Schneiderman , R. 'Cyber Skills in High Demand Well Into The Future'. Newswise, 7 Sep 2016. Accessed Dec 2016. www.newswise.com/articles/view/660345/.
4. 'Cyber-security Unemployment Rate Drops To Zero Percent'. Cyber Security Career News, Cyber Security Ventures, Q3 2016. Accessed Dec 2016. http://cybersecurityventures.com/career-news/.
5. Correa, D. '82% of global IT pros admit to a shortage of cyber-security skills'. SC Magazine, 2 Aug 2016. Accessed Dec 2016. www.scmagazineuk.com/82-of-global-it-pros-admit-to-a-shortage-of-cyber-security-skills/article/512830/.
6. 'Lack of Security Talent: An Unexpected Threat to Corporate Cybersafety'. Kaspersky Lab IT Security Risks Special Report Series 2016. Accessed Dec 2016. https://business.kaspersky.com/security_risks_report_lack_of_security_talent/.
7. 'National Cyber Security Strategy 2016-2021'. HM Government, 1 Nov 2016. Accessed Dec 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
8. 'Databarracks Data Health Check 2016 Report'. Databarracks, Oct 2016. Accessed Dec 2016. http://info.databarracks.com/DataHealthCheck2016.html.
9. 'GCHQ-certified degrees'. National Cyber Security Centre, 2 Oct 2015. Accessed Dec 2016. https://www.ncsc.gov.uk/information/gchq-certified-degrees.
10. Tittel, E; Lemons, M; Kyle, M. 'Introduction: Information security and cyber-security certifications'. TechTarget. Accessed Dec 2016. http://searchsecurity.techtarget.com/tip/SearchSecuritycom-guide-to-information-security-certifications.
11. Tittel, E. 'Best Information Security Certifications For 2016'. Tom'sIT PRO, 3 Sep 2015, Accessed Dec 2016. www.tomsitpro.com/articles/information-security-certifications,2-205.html.
12. CompTIA Security+, home page. Accessed Dec 2016. https://certification.comptia.org/certifications/security.
13. 'Certified Ethical Hacking Certification. EC-Council. Accessed Dec 2016. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/.
14. 'Security Certification: GSEC'. GIAC. Accessed Dec 2016. www.giac.org/certification/security-essentials-gsec.
15. 'Certified Information Security Manager (CISM)'. ISACA. Accessed Dec 2016. www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx.
16. 'CISSP – Certified Information Systems Security Professional'. (ISC)2. Accessed Dec 2016. https://www.isc2.org/cissp/default.aspx.
17. IISP Skills Framework Issue 2.0. The Institute of Information Security Professionals, May 2016. Accessed Dec 2016. https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/

Fighting fraud on mobile networks

Andy Gent

Andy Gent, Revector

In a recent comprehensive global survey of 150 telecommunications network operators, two issues were identified as the most significant threats to operators' revenues. One of these has already cost operators an average of 20% of their termination revenues this year. The other has been a risk for many years but continues to threaten revenues on 80% of the networks surveyed. So what are these threats and what can we do about them?

Mobile targets

Mobile network operators have long been targets for fraud and revenue risk. The