What Skills do you Need to Work in Cyber Security? A Look at the Australian Market

Leigh Ellen Potter
Griffith University
170 Kessels Road
Nathan, Queensland, Australia
+61 7 3735 5191
L.Potter@griffith.edu.au

Gregory Vickers
Griffith University
170 Kessels Road
Nathan, Queensland, Australia
+61 7 3735 4847
G.Vickers@griffith.edu.au

ABSTRACT
The demand for cyber security professionals is rising as the incidence of cyber crime and security breaches increases, leading to suggestions of a skills shortage in the technology industry. While supply and demand are factors in the recruitment process for any position, in order to secure the best people in the security field we need to know what skills are required to be a security professional in the current cyber security environment. This paper seeks to explore this question by looking at the current state of the Australian Industry. Recent job listings in the cyber security area were analysed, and current security professionals in industry were asked for their opinion as to what skills were required in this profession. It was found that each security professional role has its own set of skill requirements, however there is significant overlap between the roles for many soft skills, including analysis, consulting and process skills, leadership, and relationship management. Both communication and presentation skills were valued. A set of 'hard' skills emerged as common across all categories: experience, qualifications and certifications, and technical expertise. These appear to represent the need for a firm background in the security area as represented by formal study and industry certifications, and supported by solid experience in the industry. Specific technical skills are also required, although the exact nature of these will vary according to the requirements of each role.

Categories and Subject Descriptors
H.1.2 [**User/Machine Systems**]: Human Factors

General Terms
Security, Human Factors.

Keywords
Cyber security, skills, security professional.

SIGMIS-CPR '15, June 04 - 06, 2015, Newport Beach, CA, USA Copyright 2015 ACM 978-1-4503-3557-7/15/06···$15.00 http://dx.doi.org/10.1145/2751957.2751967

1. INTRODUCTION
The demand for cyber security professionals to protect companies from perceived threats is rising as the incidence of cyber crime and security breaches increases. Between 2012 and 2013, Australian Government departments and networks have experienced a 21 per cent increase in cyber threats (Cyber Security Operations Centre, 2014). Internationally, cyber crime has become increasingly prevalent, and is exacerbated by the prevalence of new technology and mobile technology (Symantec, 2014).

Rapid change in both the technology and security sectors means requirements for meeting the challenge are also changing. Individuals with security credentials are in increasing demand. Major companies in Australia are participating in initiatives designed to garner potential security specialists, such as the Cyber Security Challenge Australia. The FBI has described individuals with cyber expertise as it's most sought-after candidates", and is currently seeking to hire "highly talented, technically trained individuals" to become cyber agents (FBI, 2014).

The problem however is availability of talent. Part of the remit for the Cyber Security Challenge Australia 2014 was "to address a skills shortage in the number of cyber security professionals in Australia" (CySCA, 2014). A major Australian university has tried to appoint an IT Security manager for the past three years, to date unsuccessfully. Demand appears to outstrip supply.

While supply and demand are clear factors in the recruitment process for any position, in order to secure the best people in the security field we need to know what skills are required to be a security professional in the current cyber security environment. This paper seeks to explore this question by looking at the current state of the Australian Industry. We will analyse recent job listings in the cyber security area and present responses from current security professionals in the technology industry giving their opinion as to what skills are required by a security professional. Through this process we aim to generate an initial list of key skills required by a security professional.

We will present an overview of the skill situation from current literature, and then outline the approach we took for this study. The key data gathered in the study will be presented and discussed, in order to provide the security professional skill list.

2. CONCEPTS
Studies specific to the skills required by a modern security professional are sparse. Many studies exist looking at techniques and the broad technology professions, such as software

engineering or business analysis, however work looking specifically as security professional skills are few.

Palmer (2012) stresses the importance of a mix of hard and soft skills, with hard skills represented in such tasks client/desktop support, programming and PC maintenance, and soft skills identified as communication, problem solving, and decision making. He also describes the qualifications and certifications that a network security engineer should possess, describing a background in information technology, information security, networking and engineering. He lists lifelong learning in order to keep up with new technology and new security solutions as important, and outlines a basic risk management approach as crucial for this position. He considers that a network security engineer should be capable of developing security policies and business continuity and disaster recovery strategies, and be able to test their developed plans and solutions prior to implementation.

Casper and Papa (2012) argue that current security degrees focus on network security and information assurance, and that this focus leads to "serious gaps in the mentality and abilities of the security engineer, and this hole in ability results in significant holes in the armor of the security design of a system." They suggest that skills from multiple disciplines are needed to address this problem, and specifically cite the importance of skills from the usability field.

Caldwell (2013) discusses a cyber security skills gap, and while she is not explicit as to specific skills, she does discuss issues such as "a mismatch between the expectations of employers and the needs of technically skilled employees" and that organisations may need to adjust their views in order to attract the right personnel. She also raises the challenge of junior security professionals gaining the experience they need for the industry.

The Cybersecurity Workforce Competency report (University of Phoenix & (ISC)2 Foundation, 2014) acknowledges a need to standardize a "set of industry-aligned professional competencies can help in educating, recruiting, developing, and retaining the caliber of talent that the industry needs." It identifies three gaps that hinder the progress of both security professionals and the profession itself: a competency gap between the proficiency level an individual possesses and that which an organisation desires, a professional experience gap, and an education speed-to-market gap where tertiary institutions are unable to adapt subject material in line with the speed of the changing security environment.

3. APPROACH

To identify the skills needed to work in cyber security, we conducted an analysis of a set of job advertisements and deployed a questionnaire to a group of cyber security professionals. These will now be described, together with the analysis process used.

Job advertisements from a major Australian internet job site (Seek.com.au) were gathered using a keyword search of "cyber security" with no constraints on classification, location (within Australia) or salary. The search was conducted in January 2015, with listings dated from December 2014 to early January 2015. This search returned 60 job listings, which was reduced to 33 listings with the removal of duplicate listings (the same job listed in multiple categories) and non-cyber security jobs. These 33 listings came from 18 separate employers, with the majority of listings from major Australian companies, and international companies with Australian offices. One employer listed 8 individual positions. Employers represented a broad range of industries, including finance, small and large consultancy companies, and the government sector. The majority were large companies. The final 33 job listings were analysed according to the skills listed as required or desirable for the job.

A questionnaire was sent in November 2014 to a group of seven Queensland Information Technology security professionals whose core role involved ensuring the security of the information technology networks of large, complex organisations asking them to describe the skills they felt were required to work in this field. Five professionals responded. The questionnaire included four open questions, and simply asked respondents to list and describe the key technical skills and personal skills that someone would need to be a good IT security professional, and which skills they felt were most important.

Both the job listings and questionnaire responses were then analysed using the computer assisted qualitative data analysis software NVivo 10 to code each skill or characteristic in the listing or response to a theme. These themes were identified as they emerged from the data itself, resulting in a set of skills that were common across both data sets, and additional skills for specific situations. These skills will now be discussed.

4. RESULTS

The 33 job listings covered a broad range of jobs, and based on the job titles these fell broadly into six security categories: Analyst, Consultant, Engineer, Security Assessor / Advisor, Manager, and Sales. The skill requirements were analysed for each category, and while there was significant overlap between some categories, each category resulted in an individual list of required skills.

4.1 Analyst

Four full time jobs were advertised as Analyst positions. These position descriptions involved "advice and subject matter expertise to stakeholders", "problem solving skills", "supporting the team with cyber security incidents", "risk management activities" and "security related support and incident management services". In one case, a job also listed "Any other duties as required". Analysis of the job descriptions yielded nine required skills for these positions: Analysis, Innovation, Motivation, Process creation, Team Work, able to work independently, Qualifications and certifications, Experience, and Technical expertise.

Analytical skills and "a sharp eye for detail" were listed, together with "innovative skills". One job asked for someone "highly motivated with a strong sense of ownership\responsibility and a keen passion for learning". Another asked for someone capable of the "development of incident handling, detection and threat mitigation procedures", who has "experience in working in geographically dispersed teams along with being able to work independently."

The remaining three skills were listed as critical in all positions. All positions required tertiary qualifications, with a degree in computer science or related field preferred, or the equivalent combination of education and experience. Three positions asked for industry certifications, and two asked for security clearance. All positions asked for applicants with experience, either in terms of cyber security experience ("3+ years of experience supporting cyber security or information security initiatives"), or experience with specific technologies required for the job. The final skill of technical expertise is listed with the greatest amount of detail in the listings, with all listings including specific technologies, frameworks, or expertise required for the role

4.2 Consultant

Nine jobs were listed with 'Consultant' in the title in both junior and senior positions. These were described as roles involving independent work and assistance to teams, analysis and "complex technical investigations", the identification, development, and management of customer relationships and opportunities, and the development of solutions. The twelve skills listed for consultancy jobs were the ability to work independently, process skills, leadership, presentation skills, time management, risk management, analysis, communication, consulting, qualifications and certifications, experience, and technical expertise.

Working independently was stated in one listing and implied in several others as "the consultant is responsible and accountable for…" the specific tasks in the job listing. Process skills refer to the ability to either establish or follow and maintain a framework of processes and procedures that support the organisation in meeting its goals, and this was included in the job listings. The more senior consultancy positions included management and leadership skills, together with the ability to report findings in formal presentations. Several jobs required skills in risk management and security risk management, and analytical skills were highly valued as consultants needed to "use their initiative and experience to analyse, plan, review and adjust priorities and work activities to meet business outcomes." Most positions required "Excellent communication (including written and presentation skills)" regardless of the seniority of the position. Unsurprisingly, these positions asked for the "ability to consult with business and technical representatives and to balance security and business requirements."

As with analysts, the most commonly sought skills were qualifications, certifications, experience, and technical expertise. Computer Science, ICT Security related degrees, and post-graduate qualifications were an advantage, however industry certifications such as CREST (security testing), CISSP (Certified Information Systems Security Professional), and CISM (Certified Information Security Manager) certifications were more commonly requested. One role asked for "Participation and membership of relevant industry associations." All jobs asked for industry experience as either mandatory or desirable, with specific experience requested by some listings as relevant for the listed position. This varied from the more general "industry experience or knowledge" to quite specific requirements, such as "five years of professional experience", and "seasoned experience". The area of technical expertise was again the most specific, with most listings requesting specific technical skills specific to the job, such as vulnerability assessment, threat and risk assessment, and expertise with specific technologies, frameworks and standards.

4.3 Engineer

One listing for multiple positions was listed for a Security Engineer. This will still be discussed separately as the term "security engineer" is an established title: a subsequent job search was conducted using only this title with a return of fifteen job listings, which were not included in this "cyber security" analysis. The position of Security Engineer has a technical focus dealing with network security, incident response, intrusion detection, and vulnerability assessment. The listing reflects this with a focus on analytical skills, experience, qualifications, and technical expertise.

Analysis in this case is the technical analysis of elements such as network traffic and log files. A Bachelor's degree in Information Security was desirable, as were industry certifications, in this case technical certifications including Cisco and security testing together with CISSP. "Four or more years of experience in network, host, data and/or application security" was essential for this position, with experience in a very specific list of technical skills relevant to the position requested in the listing.

4.4 Security Assessor / Advisor

Ten job listings were included in the Assessor / Advisor category with a focus on security assessment and advice. This category includes roles "for conducting security assessments including penetration testing and vulnerability assessments, and design tasks". The ten key skills identified for this category include consulting, analysis, process skills, relationship management, motivation, presentation skills, communication skills, experience, qualifications, and technical expertise.

One job listed consultancy skills in order to "balance security and business requirements when managing information security incidents". Analytical skills are listed, either directly ("possess advanced analytical and problem solving skills") or indirectly ("the ability to capture and articulate testing results"). This category includes process skills, such as "following a systematic methodology" and skills in governance. Relationship management is important in terms of relationships within teams and with the client. Motivation to perform the job appears to be key, with statements such as "You will display a passion for cyber security", "a passion for security, particularly Penetration testing", and "You will be passionate about technology and willingly engage in self-learning and security research as part of your daily life." Both presentation and communication skills appear to be important in this role with inclusion in multiple listing, as clearly articulated in the criteria for "Strong presentations skills including an ability to interpret and communicate complicated topics to all levels of stakeholders" and "Excellent presentation and communication skills are a must."

As with the earlier categories, the most commonly included skills are qualifications and certifications, experience and technical expertise. Computer Science or Information Technology degrees are most commonly requested. Industry certifications are more frequently listed than tertiary qualifications, with the more general certifications such as CREST, CISSP and CISM most commonly listed. All of the job listings require experience, either generally ("3 years", "we expect you will have recent experience") or specifically ("you MUST have a strong and indepth background in Endpoint Protection"). As with previous listings, by far the most detailed requirements are for technical expertise, with all of the job listings giving specific criteria for the position. In this category, these skills primarily relate to vulnerability assessment and penetration testing, with security framework understanding and competence highly valued.

4.5 Manager

Seven jobs were listed as managerial positions including Operations manager, executive manager, and cyber security manager. These roles involved management of teams, units, or security centres and resulted in the largest number of skills, with fourteen identified from the descriptions. These are event/Incident management, presentation skills, innovation, leadership, risk management, project management, process creation, process management, consulting skills, team management, qualifications and certifications, experience, technical expertise and relationship management.

A range of management roles were included in the listings, with some requiring the management of specific scenarios, such as

"identified security events and incidents through to resolution". The ability to present to "C level executives" and "various other stakeholders" was desirable. The ability to innovate, be a "thought leader", and "bring a fresh perspective to the way we do things" was valued, as was the ability to inspire a team to "innovate and deliver value". The positions were often described as "leadership position(s)", with the ability to "influence the whole enterprise". Risk management skills were valued and listed in several positions, as were project management skills. The "demonstrated ability" to develop and maintain "key operational processes and procedures" was included in most of the positions, with both the creation of processes, and the implementation and maintenance of processes key requirements. "High level consulting" skills were listed in most of the positions, with the "ability to consult with business and technical representatives" and "the ability to advise clients, from a vendor agnostic perspective" identified as required. Perhaps not surprisingly, all but one of the listings included team management as a required skill, in terms of management of specific security operations teams, or more generally as an "experienced people leader keen to inspire, mentor and motivate large teams" or "proven people management experience."

Qualifications were only listed for three positions, with a requirement of "tertiary qualifications in Computer Science or related discipling", and "relevant industry certifications" were listed for only two positions. Three positions requested "Participation and membership of relevant industry associations." Experience appeared to be more valued, appearing in most of the job listings. In the manager category, experience in a management position and an "understanding and previous involvement with Cyber Security technologies and processes" were valued. Technical expertise was listed in all positions, however the descriptions of technical skills were more general than the other position descriptions. Skills required included a "strong level of technical security knowledge", an understanding of "security architecture and the pitfalls around different technologies", and "familiarity with modern attack systems and methodologies."

Relationship management appears to be the most valued skill in this category, appearing in every listing in a range of forms. Relationship management was included at several levels, including the management of internal teams, "maintenance of a close working relationship with other members of the client's teams", "maintaining and enhancing a good working relationship with the PSO (Principal Security Officer) Business Owners", and "managing stakeholders to effect change, including strong influencing skills."

4.6 Sales

Two job listings were sales positions: a Business Development Manager and a Security Bid/Proposal Engineer. The Security Bid/Proposal Engineering position included development of security solutions, and "working on Bids, Proposals and RFP responses." The Business Development Manager was "responsible for developing and growing a range of key Enterprise accounts" in the cyber security area. The skills listed for these positions include Innovation, presentations skills, relationship management, communication, certifications, experience, and technical expertise.

The manager position listed an "innovative, lateral and pragmatic thought process" as a requirement. Both positions included the ability to present ideas. The manager position also included "exceptional relationship management" and "negotiation" skills as required. Both jobs required communication skills, with the manager position listing the "ability to communicate to all levels of key stakeholders" and the engineer position citing "strong writing and oral skills".

Only the engineer position requested formal qualifications, stating that an applicant should be a "Certified Information Systems Security Professional." Experience was more valued in both positions, with sales experience listed for both roles. The manager position asked for "an understanding of security, hacking or cyber espionage", but also stated that "a background in Security Software is an advantage but not essential." The engineer position requested specific security experience, as well as "experience supporting proposal development and capture activities." Specific technical expertise was required for the engineer position, with a list of general security skills such as intrusion detection, log monitoring, and security management and reporting listed.

4.7 Skills identified in Questionnaires

The skills identified in the questionnaire responses were not targeted at an identified position, and included both general and specific skills. These included the ability to learn, leadership, management, problem solving, communication, the ability to deal with people, analysis and motivation. These responses also included experience and technical expertise.

"Drive and the ability to learn" was cited as a valuable skill, as was the ability to inspire and lead. Management was seen as important, with one response in particular listing "PM skills, time management, vendor management, management management (seriously!)." For a security professional, "problem solving is key", with both research and analysis included as required skills. Communication is vital, with a requirement for the "ability to present data and reports to middle and senior management, with a business focus, without getting lost in the minutia of IT Security", and the "ability to communicate with people in a clear manner - when talking with a user, a manager, or a senior manager, the message has to be clear and well understood."

The ability to deal with people was clearly identified, with responses stating that a security professional should "get along with people", and have "the ability to interact with a user or users when establishing the situation that you are investigating - this has to be a respectful and honest conversation." Analytical skills were important to making this happen, as accurate information informs these relationships. The most commonly listed analytical skills given in the responses were technical, in terms of "log management and investigation into that data", and the "ability to integrate data from many sources and provide a reasonable, evidence based summary."

The motivation of the individual was seen as important for a security professional. Responses listed attributes such as being "hungry to learn anything and an independent learner", "drive and the ability to learn", and "curiosity" as important, as was someone who "wants a deeper understanding of how attacks/defense work."

While formal qualifications or certifications were not included in the questionnaire responses, both experience and technical expertise were. Responses included skills such as "a broad knowledge of networking, storage, system administration", "log data management and investigation into that data", and the "ability to integrate data from many sources and provide a reasonable, evidence based summary." One response was very specific, citing "Strong experience in two or more of the

following: Coding/Scripting, Network Management, Server Administration (Windows and Linux), and Management of Core Services (DNS,Mail, DBA, ect..)" as important.

4.8 Security Professional skills

A set of skills suitable for six categories of Security Professional emerged as the job advertisements were analysed. Analyst positions needed nine skills: Analysis, Innovation, Motivation, Process creation, Team Work, able to work independently, Qualifications and certifications, Experience, and Technical expertise. Consultants needed twelve skills: the ability to work independently, process skills, leadership, presentation skills, time management, risk management, analysis, communication, consulting, qualifications and certifications, experience, and technical expertise. An engineer requires analytical skills, experience, qualifications, and technical expertise, however this list is limited by the single job listing analysed. Security advisors and assessors need ten key skills: consulting, analysis, process skills, relationship management, motivation, presentation skills, communication skills, experience, qualifications, and technical expertise. Managers require the largest skillset with fourteen listed: event/Incident management, presentation skills, innovation, leadership, risk management, project management, process creation, process management, consulting skills, team management, qualifications and certifications, experience, technical expertise and relationship management. Sales positions included seven skills: innovation, presentations skills, relationship management, communication, certifications, experience, and technical expertise.

Analysis of the questionnaire results revealed that current security professionals view eleven skills as core to the profession: the ability to learn, leadership, management, problem solving, communication, the ability to deal with people, analysis and motivation. These responses also included experience and technical expertise.

These skills represent a blend of both soft skills and technical skills. Soft skills that were included in many job listings across the categories included analysis, consulting skills, leadership, process skills, and relationship management. Both communication skills and presentation skills were valued. Experience and technical skills are critical, and included in all job listings and the questionnaire responses. The specific technical skills vary, depending on the characteristics of the job, however it is interesting to note that these were still cited in the questionnaire responses even though these responses were not addressing a specific position.

While not mentioned in all categories, motivation to do the job appears to be a valued trait. "Highly motivated", a "keen passion for learning", a "passion for cyber security", "passionate about technology", and a willingness to make "self-learning and security research as part of your daily life" were all listed in different job advertisements. In questionnaire responses, attributes such as "hungry to learn", "drive" and "curiosity" were all discussed. This reflects findings by Potter, von Hellens, and Nielsen (2009) suggesting that motivation is a key driver for an individual to both enter and remain in the Information Technology profession.

4.9 What's in a name?

In searching for jobs with the general search term of "cyber security", and in gathering responses from security professionals currently working in the IT industry, we observed a phenomenon that occurs in some other IT industries such as within information systems and the user experience field. Terms and labels for positions within the security field can be ambiguous, with different labels applied to very similar positions. Very few of the 33 job advertisements that we analysed had the same job title: we saw eighteen separate job titles advertised within this simple search. In some cases the same role was advertised with very different titles: for example, the titles penetration tester, security assessor, risk consultant, and security advisor were all used for a role that fit the description of penetration tester.

This was reflected in the diverse job titles of the questionnaire respondees, with Security Engineers, Security Specialists, and Security Project Manager among the titles given, despite all questionnaire responses coming from people tasked with very similar roles. The problem appears to not just be a variety of different names, but also the understanding of specific titles. One response stated that "a Security Engineer in one organisation could have a vastly different role to that at another." Confusion around the naming of roles within the security sector further complicate the question of skill requirements.

5. CONCLUSION

This paper asked what skills does a security professional need in the current information technology environment, and explored this question by looking at the current state of the Australian industry. Recent job listings in the cyber security area were analysed, and current security professionals in industry were asked for their opinion as to what skills were required in this profession.

It was found that each security professional role has its own set of skill requirements, however there is significant overlap between the roles for many soft skills. Analytical and consulting skills were valued as supporting interaction with clients, processing of complex data, and provision of the information generated back to the client. Leadership skills were valued as a means of dealing with other security specialists and promoting security work. The ability to create a process or procedure was valued for senior roles, and the ability to follow an established process or procedure was valued for many roles. Relationship management was seen as an important skill, supporting the interaction of the security professional with peers, clients, and senior management. The questionnaire responses took this a step further to suggest that security professionals need to be able to manage many competing demands, including time, priorities, and the technical aspects of the role.

Security professionals need to be good communicators, and many roles require the applicant to be able to present their ideas and findings in a formal setting. The ability to communicate was further emphasized in the questionnaire responses, with the ability to deal with people and an enthusiasm to learn was highly valued.

A set of skills emerged as common across all categories: experience, qualifications and certifications, and technical expertise. These appear to represent the core 'hard' skills of all security professionals, in terms of a solid background in the area as represented by formal study and industry certifications, and supported by solid experience in the industry. Specific technical skills are also required, although the exact nature of these will vary according to the requirements of each role.

6. REFERENCES

[1] Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5–10.

[2] Casper, W. D., & Papa, S. M. (2012). A Multi-Disciplined Security Engineering Education Approach. In *SAM 2012* (pp. 243–248).

[3] Cyber Security Operations Centre. (2014). *The Cyber Security Picture 2013*. Canberra, ACT.

[4] CySCA. (2014). Cyber Security Career Opportunities.

[5] FBI. (2014). Most Wanted Talent: FBI Seeking Tech Experts to Become Cyber Special Agents. Retrieved December 31, 2014, from http://www.fbi.gov/news/stories/2014/december/fbi-seeking-tech-experts-to-become-cyber-special-agents

[6] Palmer, I. (2012). How to become a network security engineer. *Infosec Institute*. Retrieved from http://resources.infosecinstitute.com/network-security-engineer/

[7] Potter, L. E. C., von Hellens, L. A., & Nielsen, S. H. (2009). Childhood interest in IT and the choice of IT as a career. In *Proceedings of the special interest group on management information system's 47th annual conference on Computer personnel research - SIGMIS-CPR '09* (p. 33). New York, New York, USA: ACM Press. doi:10.1145/1542130.1542138

[8] Symantec. (2014). *2013 Norton Report* (p. 28).

[9] University of Phoenix, & (ISC)2 Foundation. (2014). *Cybersecurity Workforce Competencies: Preparing tomorrow's risk-ready professionals* (p. 16).