https://doi.org/10.48009/2_iis_2019_62-72

Issues in Information Systems
Volume 20, Issue 2, pp. 62-72, 2019

WHAT IS CYBERSECURITY AND WHAT CYBERSECURITY SKILLS ARE EMPLOYERS SEEKING?

Alan Peslak, Penn State University, arp14@psu.edu
D. Scott Hunsinger, Appalachian State University, hunsingerds@appstate.edu

ABSTRACT

With nearly 100% of our world's information stored on computers and databases, the threat of compromising this information looms as arguably the most critical risk that we must deal with as a global society. Rising from this threat is a critical need for cybersecurity experts. But what exactly cybersecurity is and what skills are required from employers today is unclear. Our research explores a variety of sources for a clearer picture of the cybersecurity landscape, the threats, the definition, and the areas of concern. In addition, we analyzed job descriptions from nearly 500 ads to determine the specific and general skills that are expected from cybersecurity analysts and professionals. Our study determined that cybersecurity, in general, is the protection of data, information, devices, and systems from unauthorized or malicious attacks or access. The requirements that employers are seeking were found to be general technical skills and experience related to cyber threats and in lesser numbers, specific skills in cybersecurity technology or vendor products.

Keywords: Cybersecurity, information security, security, privacy, risk management, CISSP

INTRODUCTION

The security of personal information has never been more important and potentially more vulnerable. In 2017, there were seven major data breaches that exposed personal data for millions of individuals. Overall, it was estimated that there were more than 1,500 data breaches in 2017, a 37% increase over prior year. The Equifax breach led the way with exposure of 143 million Americans' social security numbers, birthdays, addresses and other information. In this breach, 209,000 individuals' credit card data were released as well. Uber incurred a breach that affected 50 million customers. Edmodo, a social learning platform exposed data from 77 million users. Verizon had 14 million of their customers' data exposed. Deep Root Analytics, a voter analytics company, exposed data from 198 million voters (Strain, 2018).

In 2018, things got worse. In India, Aadhar, which stores demographic and biometric data for Indian citizens, was hacked, leaking names, bank accounts and other information for 1.1 billion people. Marriott Starwood was compromised, releasing detailed guest information including credit cards for 5 million customers. Exactis, a marketing data aggregator exposed 340 million consumers' data. MyFitnessPal was hacked and exposed 150 million individuals. Quora, a popular question answering source, exposed 100 million members' data. (Salim, 2019)

The list goes on and on. Clearly, the security of our data is at major risk. To respond to this risk a new discipline has been created in the computing world. This discipline is cybersecurity. But the definition of cybersecurity and the skills required for this discipline are unclear. This manuscript is an initial effort to explore and define cybersecurity by reviewing current sources for definitions but also by examining the skills that are expected of cybersecurity analysts in today's marketplace. The importance of clarifying cybersecurity and its skills can have significant impact on improving privacy and security in the world.

Cybersecurity Definitions

With nearly 100% of our world's information stored on computers and databases, the threat of compromising this information looms as arguably the most critical risk that we must deal with as a global society. Rising from this threat is a critical need for cybersecurity experts. But what exactly cybersecurity is and what skills are required from employers today are not clearly defined.

Craigen, Daikun-Thibault, & Purse (2014) were one of the first to recognize that cybersecurity is an ill-defined term. They note, **"**Cybersecurity is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges."

There are many definitions of cybersecurity, the risks that are involved, and the importance of various factors. A major cybersecurity software vendor, Kaspersky Labs (2019), defines it thus:

"Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories."

The first step in understanding the definition of cybersecurity is to examine what it attempts to do: namely defend data from malicious attacks. The next piece of the definition is what needs to be defended. With the proliferation of data and control devices and the expansion of Internet of Things (IoT), the areas that need to be protected include all connected devices, as well as all independent systems or data. Clearly, computers, servers, mobile devices, networks, and databases fall under this comprehensive definition but now all electronic and non-electronic devices that control any device including but not limited to cars, refrigerators, toasters, RFID chips, smart homes, bike locks, door locks, smart speakers etc., need protection from malicious attacks. This is the expanded world of cybersecurity today.

Kaspersky notes six general domain areas that are included in cybersecurity:

"Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization."

Craigen, Diakun-Thibault, and Purse (2014) performed a comprehensive literature review and propose the following definition for cybersecurity. "*Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign* de jure *from* de facto *property rights."* This is a bit of an esoteric definition, but in essence what we believe they are

suggesting, is that cybersecurity includes the application of all resources and activities protecting property rights (theft, privacy, destruction, alteration, and/or reproduction) in electronics, devices or networks.

Wulf and Jones (2009) in a prestigious Science journal suggest three areas for cybersecurity

1. The current common model is noted to be "perimeter defense", or keeping your data protected from outside attackers;
2. They add however the cybersecurity threat of insider attackers or misuse of information within an organization itself;
3. They also add the concept of "defense in depth" or a multiple level of defense of other systems once a perimeter defense has been breached.

LITERATURE REVIEW

Many past studies have been performed to analyze skill sets necessary for the IT job market. These studies have been useful in understanding how the needs of industry have changed over time, particularly with respect to technical skills.

Even though the focus of this paper is on cybersecurity skills, it is helpful to first review older studies that have examined general IS job advertisements. Later research has examined specific types of IS-related positions, including those related to programming, data analytics, and networking. Several recent articles have begun to analyze cybersecurity job postings.

Todd, McKeen, and Gallupe (1995) compared the content of IS job advertisements from 1970 to 1990. They looked at three job types: Programmers, systems analysts, and IS managers. During this timeframe, they discovered that the biggest changes occurred in the specified job requirements for systems analyst positions.

Nord and Nord (1995) identified information technology skills in the categories of technical, systems, managerial, and business by surveying a group of analysts.

Koong, Liu, and Liu (2002) selected two Internet job databases, Monster.com and HotJobs.com, to gather data and classify skills into five categories: Programming languages, web development, database, networking, and operating system environments. They extracted 150 jobs from each database to analyze skills required for each category.

Fang, Lee, and Koh (2005) conducted a national study of the perceptions of IS recruiters.

Litecky, Aken, Ahmed, & Nelson (2010) used a web content mining approach to analyze almost 250,000 unique IT job descriptions from multiple job search engines. They identified 20 categories of computing jobs and the skills needs associated with these.

Kim and Lee (2016a) developed a Web crawler to collect approximately 140,000 job postings over a year from 11 countries. They suggested that an improved classification approach is necessary in order to better categorize job advertisements, as the pre-defined job categories provided by Niederman et al. (2016) are not sufficient.

Park, Jun, and Kim (2015) used online job postings from monster.com and jobkorea.co.kr to analyze differences between US and South Korea skills requirements of IS consultants. They discovered that over half of the US advertisements required a Bachelor's degree vs. 21% in South Korea. They also found that specialized certifications such as CISSP, CISA, CISM, and GIAC were required in more than half of the job postings on monster.com and over one-third of the ads on jobkorea.co.kr.

Lee and Han (2008) conducted an analysis of skills requirements for an entry-level programmer analyst.

Gallagher, Kaiser, Simon, Beath, and Goles (2010) studied soft skills and technical skills required for programmer analysts.

Peslak et al. (2018) analyzed 500 job descriptions for programmer analyst positions posted in February 2018 on postjobfree.com to determine the most important skills, degrees, and amount of experience required for most positions. They also tabulated the languages mentioned in these postings, finding that SQL, .NET, and C# were included in many of the advertisements.

Morris, Fustos, and Haga (2018) collected data from approximately 700 job advertisements on Dice.com that related to skills required for network administration positions. Instead of soft skills, their study focused on technical skills, which were broken into categories such as virtualization technologies, scripting languages, and routing protocols. They found that some positions require networking certifications from vendors such as Cisco Systems, Microsoft, and Juniper as well as vendor-neutral certifications such as Network+ from CompTIA.

Kim and Lee (2016b) conducted a content analysis of 1,240 job advertisements from companies recruiting data scientists. Their findings showed that data scientists are expected to possess a high level of experience along with advanced academic degrees.

Verma, Yorov, Lane, and Vurova (2019) also conducted a content analysis of job advertisements for business and data analytics positions including business analyst, data analyst, data scientist, and business intelligence analyst. They observed that technical skills including programming and statistics are in highest demand for data analytics, while structured data management, organization, and communication are important soft skills for all related positions.

Potter and Vickers (2015) examined cybersecurity skills required for positions in Australia. They found that technical expertise, certifications, and experience emerged as common requirements across most job postings, in addition to soft skills including presentation and communication skills.

Benslimane, Yang, and Bahli (2016) conducted a content analysis of 100 job postings related to information security analysts and managers. Their research showed that companies value professional certifications over knowledge of specific security standards. Knapp, Maurer, and Plachkinova (2017) also noted that cybersecurity positions are more likely to require certifications than jobs in other IS areas. Approximately 35% of cybersecurity job postings mentioned one or more related certifications. Companies who hire cybersecurity professionals often look for certifications in order to assess a job candidate's overall credentials.

Brooks, Greer, and Morris (2018) analyzed approximately 800 job advertisements relating to information systems security positions in order to review the skills required for these jobs along with certification and degree requirements. They also examined the implications for information systems curricula. Domain-related skills made up 16 of the top 20 skills, including terms related to networks, standards, and policies.

Parker and Brown (2019) looked at 196 unique job advertisements from five job portal websites relating to cybersecurity. This study was restricted to requirements for positions in South Africa. They conducted a content analysis of the listings to discover that both technical and interpersonal skills are necessary. Most positions required a Bachelor's degree along with industry-specific certifications.

METHODOLOGY

The authors reviewed job postings in April 2019 from the website https://www.postjobfree.com/. This website was used instead of, perhaps, more familiar sites, such as indeed.com, because its terms of service have no restrictions and are 100% public. Indeed.com and other job sites have very specific restrictions that prevent the extraction of data and threaten legal actions, if data are extracted. Postjobfree.com has no such restrictions. This site allows you to search a job title and then returns up to 500 open jobs and their descriptions.

The authors entered "Cybersecurity Analyst" as the search term and obtained 487 non-duplicate returned job descriptions for cybersecurity analyst. Postjobfree.com includes job postings world-wide with a primary focus on the United States. Although the site allows for geographic specification, this was not entered to allow for geographic dispersity.

RESULTS

A variety of tools and analyses were used to examine the content of the job postings. Figure 1 displays a word cloud of all the postings.

Figure 1. Word Cloud

The word cloud from Voyant tools shows the relative importance of key words in the text of all the cybersecurity positions studied. With few exceptions, the words used within these job descriptions can be applicable to any technical job description. Terms such as requirements, support, knowledge, solutions, technology, design, compliance etc. all have applicability to engineering or technical careers. There are few terms that would specifically suggest a cybersecurity role, of course except for security and cybersecurity itself. This is an interesting result, since it suggests that the role of cybersecurity has more in common with other technical job requirements than with specific cyber/computer skills.

Despite the lack of specific skills within the highest frequency word cloud, there were many specific items that were included in many ads. The next series of tables reflect the 3-word, 2-word, and 1-word terms that were included in job descriptions that reflect more specific computer, risk, and cybersecurity related skills.

Table 1. Trigram Frequency Summary

Trigram Phrase	Frequency
years of experience	232
risk management framework	126
management framework rmf	100
in computer science	85
bachelor s degree	84
2 years of	66
hardware and software	60
written communication skills	57
5 years of	56
8 years of	52

Trigram Phrase	Frequency
3 years of	50
10 years of	49
nist sp 800	45
certification and accreditation	44
bachelor's degree in	43
oral and written	43
4 years of	41
of hands on	41
computer science information	40
ba or bs	39

Table 2. Bigram Frequency Summary

Bigram phrase	frequency
risk management	266
information assurance	219
computer science	162
communication skills	129
system security	128
security clearance	126
framework rmf	108
project management	106
network security	105
security requirements	104
bachelor's degree	98
5 years	96
bachelor s	95
it security	93
operating systems	90
systems engineering	88
10 years	76
dod 8570	75
3 years	74
8 years	73
software development	67
written communication	64
4 years	59

Bigram phrase	frequency
risk assessment	58
security policies	56
problem solving	55
cybersecurity policy	53
penetration testing	53
level ii	53
bs degree	53
security engineering	52
ts sci	51
sp 800	49
intrusion detection	47
vulnerability management	47
6 years	47
analytical skills	46
nist sp	45
data protection	44
security certification	44
800 53	43
system administration	41
master s	41
or bs	40
7 years	40
ba or	40

Table 3. Word Frequency Summary

Word	Frequency
security	3228
cybersecurity	1851
cissp	186
infrastructure	179
cloud	175
c	171
networks	169

Word	Frequency
linux	143
networking	136
microsoft	88
siem	78
splunk	73
cism	71
python	65

Word	Frequency
giac	63
firewall	62
unix	58
abis	56
stigs	55
ceh	53

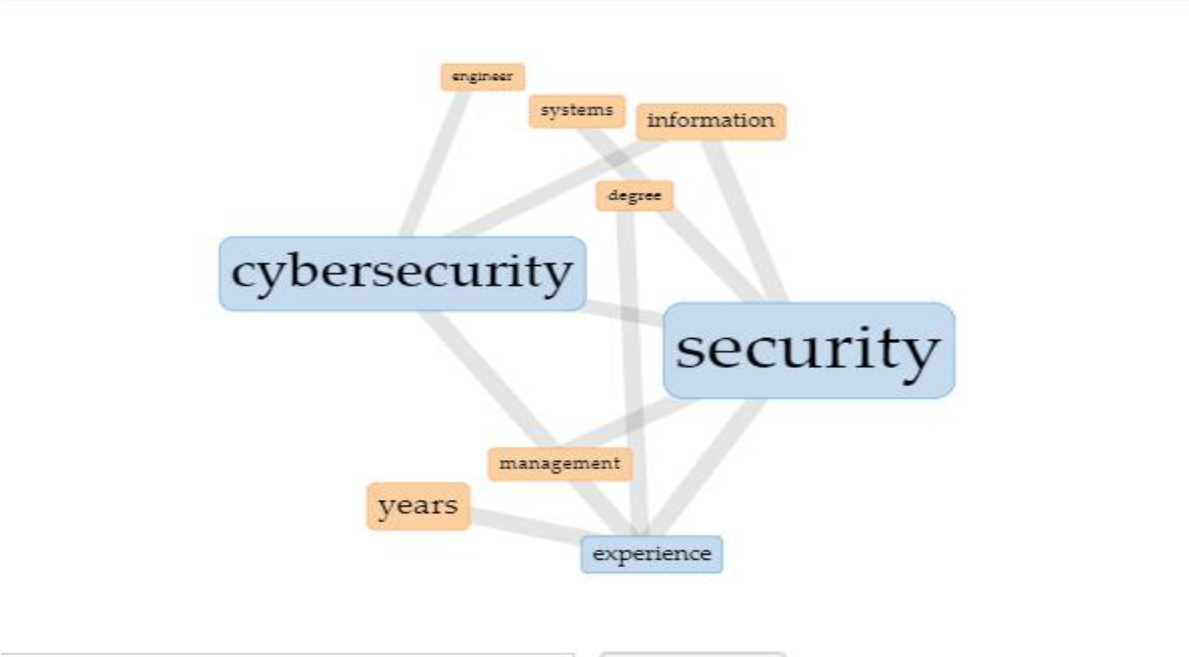

Figure 2. Collocation Chart

The collocation chart in Figure 2 shows major terms and the most common terms associated with those keywords. The major keywords in the document are security, cybersecurity, and experience. The key extracted themes include management of security and cybersecurity and years of experience with security and cybersecurity. Another term collocated with experience is degree. A degree coupled with experience appears to be a preferred combination. Associated terms with security also include information and systems. Clearly, there are specific needs to protect both information as well as overall systems. An interesting association is cybersecurity and engineer, suggesting that the field of cybersecurity is gaining the reputation as a specific engineering discipline in and of itself.

There is an interesting disconnect between many key terms and skills that are listed in 16 cybersecurity terms that everyone should know (Cyber Intelligence, 2018) and job postings. With the exception of software and cloud, most do not include or address these key terms. These suggests that either organizations assume that their candidates will know, understand, and be able to apply security concepts to this area or that they are not clear enough in their job descriptions. The sixteen terms are Cloud, Software, Domain, Virtual Private Network, IP Address, Exploit, Data Breach, Firewall, Malware, Virus, Ransomware, Trojan Horse, Worm, Bot, DDoS or DoS, Phishing or Spear Phishing. The counts of these terms are displayed in Table 4.

Table 4. Word Counts for Key Terms

List	Trend	Count
1	cloud	175
2	software*	467
3	domain	56
4	vpn*	30
4	virtual private*	5
5	IP Address	0
6	exploit*	43
7	data breach*	4
8	firewall*	128
8	firewall	62
9	malware	63
10	virus*	22
11	Ransomware	0
12	trojan*	1
13	worm*	1
14	bot	1
14	botnets	1
15	Ddos/DoS	0
16	phishing	20

Years of experience is very important with the following years cited in the job descriptions. Two hundred and thirty two descriptions did have a specific requirement of experience with 5 and 10 years being the most frequent requirements as shown in Table 5. Interestingly, just the word experience was mentioned 2341 times. So, experience is extremely important for cybersecurity analysts.

Table 5. Years of Experience Listed in Job Descriptions

Years of experience	Frequency
5	96
10	76
3	74
8	73
4	59
6	47
7	40
Total with years of experience	232
Experience	2341

Specific Skills Found Definitions

Finally, we found some specific skills that were included in many job ads and further clarify the skills needed by many employers for cybersecurity analysts. These skills require explanation.

CISSP stands for Certified Information Systems Security Professional and is a certification program offered by $(ISC)^2$ and is mentioned 186 times and is therefore one of the most sought-after technical skills. Three other certifications were prominent. CISM (Certified Information Security Manager) offered by ISACA was mentioned 71 times, GIAC (Global Information Assurance Certification) was noted 63 times and CEH (Certified Ethical Hacker) was included 53 times. NIST SP 800 was specifically mentioned 45 times. This refers to the National Institute of Standards and Technology US Dept of Commerce and their published, systematic, and codified approach to "safeguarding measures for all types of computing platforms" (National Institute of Standards and Technology, 2017) DOD 8570 had 75 mentions. This is a certification program from the US Department of Defense to ensure specific adherence to their information assurance and risk management processes. (What is DoD 8570?, 2019) Ts sci cited 51 times is Top secret government clearance and sensitive compartmented information. Siem is an acronym standing for Security information and event management and is a concept that connects information management and monitoring with active steps to address problems or issues in this realm, when required. (Rouse, 2019) The requirement was included 78 times. Other DoD terms included Automated Biometric Identification System (ABIS) 56 times and Security Technical Implementation Guides (STIGs) mentioned 55 times.

The highest noted vendors mentioned were Microsoft (88) and Splunk (73) but also included were EndPoint (51), Nessus (47) and Wireshark (28). Programming languages included were C (171) and Python (65). Operating systems noted Linux (143) and Unix (58).

CONCLUSIONS AND FURTHER STUDY

Overall, this manuscript is a preliminary investigation into the meaning and needs of cybersecurity in today's information environment.

Some significant initial conclusions from our study include:

- Cybersecurity is a multi-faceted domain area which must be dealt with in a comprehensive approach.
- General technical skills are the most often cited needs for cybersecurity analysts.
- Specific skills are needed and expected in many areas but are varied and not uniform.
- CISSP, CISM, and GIAC certifications are considered important with 185, 71, and 63 mentions respectively.
- Years of experience required by employers varies but experience is expected and is one of the most important needs of organizations today. A degree is also commonly expected.

Further research can be undertaken to further refine and understand the evolution of cybersecurity and the educational programs needed to train future leaders in the protection of our vital information. We look forward to further expanding this study.

REFERENCES

Benslimane, Y., Yang, Z., & Bahli, B. (2016). Information Security between Standards, Certifications and Technologies: An Empirical Study. 2016 International Conference on Information Science and Security.

Brooks, N., Greer, T., & Morris, S. (2018). Information systems security job advertisement analysis: Skills review and implications for information systems curriculum. *Journal of Education for Business, 93*(5), 213-221.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Cyber Intelligence (2018) 16 Cyber Security Terms That Everyone Who Uses A Computer Should Know https://www.cybintsolutions.com/16-cyber-security-terms-that-you-should-know/

Fang, X., S. Lee, & S. Koh. (2005, Fall). Transition of Knowledge/Skills Requirement for Entry-Level IS Professionals: An Exploratory Study Based on Recruiters' Perception, *Journal of Computer Information Systems,46*(1), 58-70.

Forrest, C. (2016). Obama seeks $19B for cybersecurity in 2017, a 36% increase https://www.techrepublic.com/article/obama-seeks-19b-for-cybersecurity-in-2017-a-36-increase/

Kaspersky Labs (2019) What is Cyber-Security? https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kim Y.S., Lee C.K. (2016b) An Empirical Evaluation of Job Classification Using Online Job Advertisements. In: Kang B., Bai Q. (eds) AI 2016: Advances in Artificial Intelligence. AI 2016. Lecture Notes in Computer Science, vol 9992.

Kim, J. & Lee, C. (2016a). An Empirical Analysis of Requirements for Data Scientists Using Online Job Postings. *International Journal of Software Engineering and Its Applications, 10*(4), 161-172.

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education, 28*(2), 101-114.

Koong, K. S., Liu, L. C., & Liu, X. (2002). A Study of the Demand for Information Technology Professionals in Selected Internet Job Portals. *Journal of Information Systems Education, 13*(1), 21-28.

Lee, C. K. & Han, H. -J. (2008). Analysis of Skills Requirement for Entry-Level Programmer/Analysts in Fortune 500 Corporations. *Journal of Information Systems Education, 19*(1), 17-28.

Morris, G., Fustos, J. & Haga, W. (2018). Connecting the Dots and Nodes: A Survey of Skills Requested by Employers for Network Administrators. *Information Systems Education Journal, 16*(1), 4-12.

National Institute of Standards and Technology (2017) Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

Niederman, F., Ferratt, T.W., & Trauth, E.M. (2016). On the co-evolution of information technology and information systems personnel. *SIGMIS Database, 47*(1), 29–50.

Nord, G. D., & Nord, J. H. (1995). Knowledge and skill requirements important for success as a systems analyst. *Journal of Information Technology Management, 6,* 47-52.

Park, S., Jun, H. –J, & and Kim, T. –S. (2015). Using Online Job Postings to Analyze Differences in Skill Requirements of Information Security Consultants: South Korea versus United States. PACIS 2015 Proceedings, 111.

Parker, A. & Brown, I. (2019). Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. In: Venter H., Loock M., Coetzee M., Eloff M., Eloff J. (eds) Information Security. ISSA 2018. Communications in Computer and Information Science.

Peslak, A., Kovalchick, L., Kovacs, P., Conforti, M., Wang, W., & Bhatnagar, N. (2018). Linking Programmer Analyst Skills to Industry Needs: A Current Review. Proceedings of the EDSIG Conference.

Potter, L. & Vickers, G. (2015). What Skills do you Need to Work in Cyber Security? A Look at the Australian Market. SIGMIS-CPR'15, June 4–6, 2015, Newport Beach, CA, USA. 67-72.

Rouse (2019). Security and Event Management https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

Salim, S. (2019). Revealed: The biggest data breaches of 2018. https://www.digitalinformationworld.com/2018/12/biggest-data-breaches-of-2018.html

Strain, L. (2018). The seven most colossal data breaches of 2017 https://blog.malwarebytes.com/cybercrime/2017/12/the-seven-most-colossal-data-breaches-of-2017/

Todd, P., McKeen, J., & Gallupe, R (1995). The Evolution of IS Job Skills: A Content Analysis of IS Job Advertisements from 1970 to 1990. MIS Quarterly, 19(1), 1-27.

Verma, A., Yurov, K., Lane, P. & Yurova, Y. (2019). An investigation of skill requirements for business and data analytics positions: A content analysis of job advertisements. *Journal of Education for Business, 94*(4), 243-250.

Voyant Tools (2019). www.voyant-tools.org

What is DoD 8570? (2019). https://resources.infosecinstitute.com/what-is-dod-8570/#gref

Wulf, W. A., & Jones, A. K. (2009). Reflections on cybersecurity. *Science*, 326.5955, 943-944.