Cybersecurity: Building the Workforce Rather Than Paying the Ransom

James Fong
Chief Research Officer, UPCEA
Director, UPCEA Center for Research and Strategy

Zachary Kugel
Research Assistant, UPCEA

Maria Lucchi
Research Assistant, UPCEA

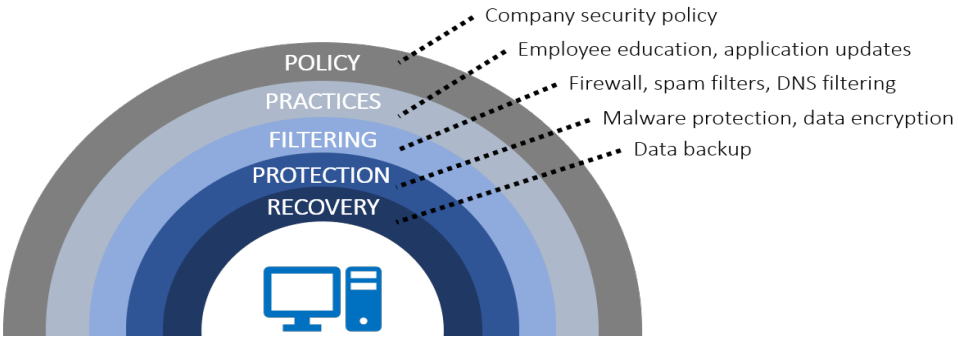
July 2019

Overview

What is Cybersecurity and Why is it Important for Higher Education?

Cybersecurity is the collection of processes and practices designed to protect the integrity of networks, programs, devices, and data from an attack, damage, or unauthorized access.[1] Sometimes, it may be referred to as information technology (IT) security. The core function of cybersecurity is to protect systems and information from cyberthreats.[2] As seen in Figure 1, strong security protocols contain multiple layers of protection distributed throughout networks, programs, and devices.[3]

Figure 1: Multiple Layers of Cybersecurity Protection[4]



Source: CSO, 2018
Source: Software Security Solutions, 2016

Three areas require protection: endpoint devices, networks, and cloud. An endpoint device is any device that can access the Internet, including computers, smart phones, and printers. When a group of these devices are physically or wirelessly connected, a network is formed. A cloud is a computer system, such as a data center, that is available to numerous users through the Internet. Google's suite of products are an example of cloud computing, as users can access files and applications hosted by Google, like Gmail and Google Drive, using the Internet. Common forms of cyber defense include firewalls, malware protection, and email security.

With ransoms being paid by system owners held hostage, attacks are likely to increase as nefarious individuals see this as a revenue stream. Higher education has a choice to make regarding the problem:

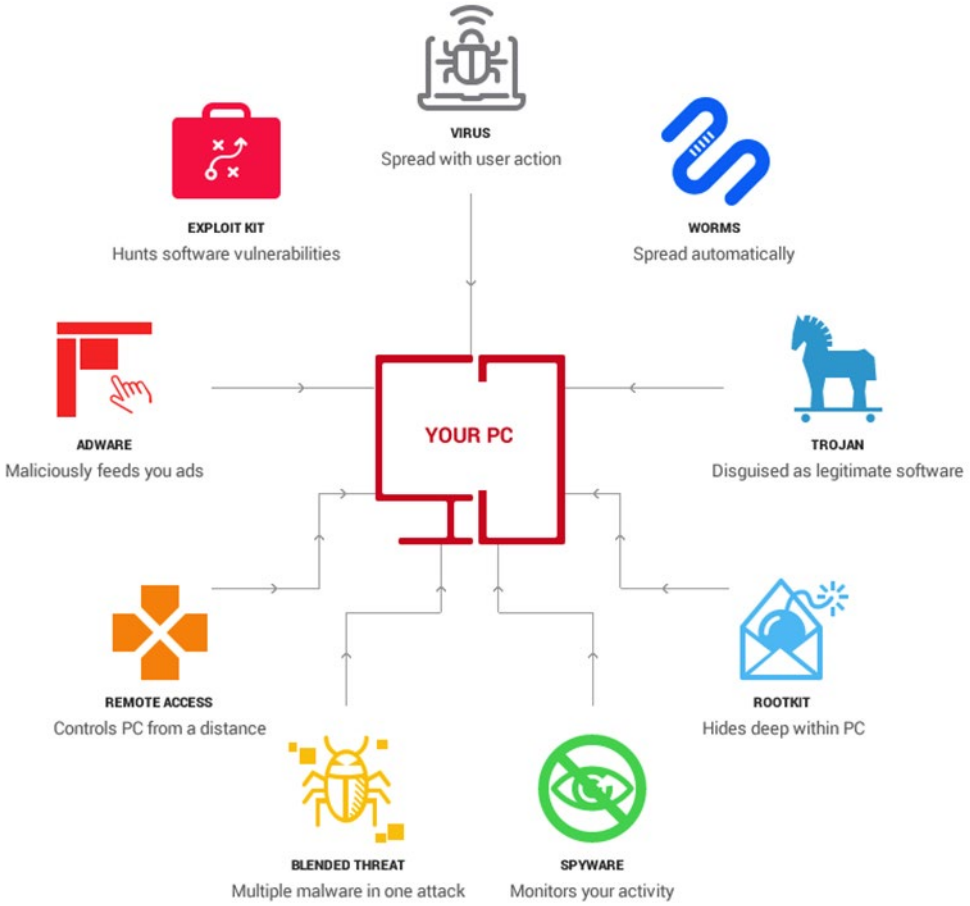
- Take a leadership position by helping to develop more cybersecurity professionals.
- Take a wait and see approach by following the lead of corporations and private industry to create solutions.

[1] https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security
[2] https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html
[3] https://www.csoonline.com/article/3326301/a-layered-approach-to-cybersecurity-people-processes-and-technology.html
[4] http://www.softwaresecuritysolutions.com/layered-security-for-business.html

- Partner with industry leaders in cybersecurity education to deliver content and bring more cybersecurity professionals to the forefront.

Firewalls are a barrier between a trusted internal network and an untrusted external network, most often the Internet. Using predetermined rules, firewalls monitor and control incoming and outgoing network traffic and are often considered the first line of digital defense.[5] A firewall can be thought of as a gatekeeper, letting through the traffic that meets predetermined criteria and blocking traffic that may be dangerous.[6] Malware is short for malicious software and is the catch-all term for any software designed to access, attack, or damage a computer. Malware protection encompasses antivirus software and further protects from trojans, worms, ransomware, spyware, among other threats that may be classified as malware.[7]

Figure 2: Types of Malware



Source: Heimdal Security, 2017

[5] https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

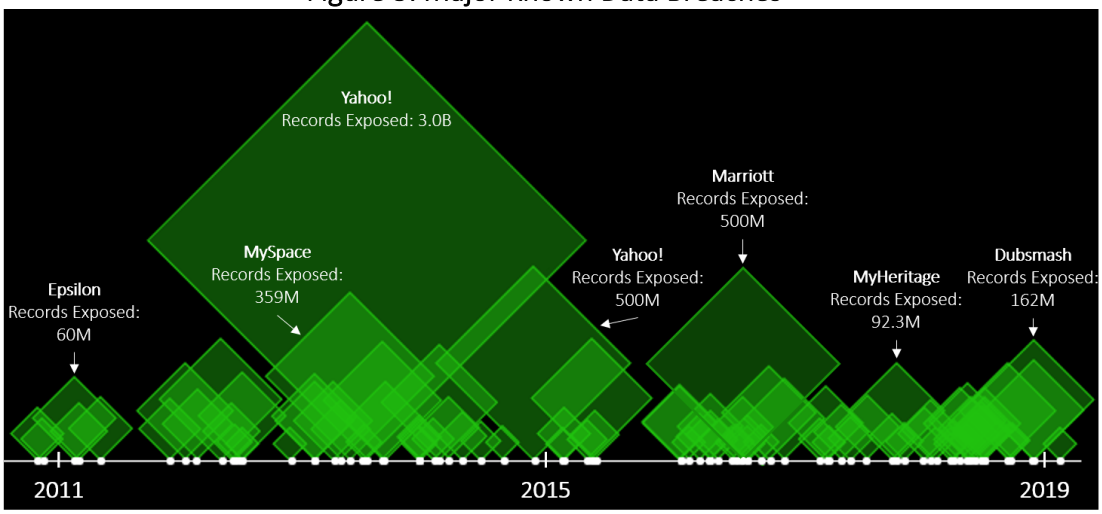
[6] https://kb.iu.edu/d/aoru

[7] https://www.webroot.com/us/en/resources/tips-articles/what-is-malware-protection

Why Does Cybersecurity Matter?

Practicing strong cybersecurity is essential as governments and corporations, as well has higher education electronically collect, process, and store unprecedented amounts of sensitive data. Today, personal devices and networks contain massive quantities of information where unauthorized access has the potential for detrimental consequences. Data sought by cybercriminals include personal, medical, and financial information, as well as intellectual property. Furthermore, governments are targeted by those seeking information relating to national security.[8] Targets of cyberattacks can include individuals, groups, corporations, and governments, including higher education. The largest known cyberattack to date occurred in 2013 when all 3 billion user accounts on Yahoo! were breached by hackers. Most recently, hackers have concentrated their efforts on local and regional governments, those who may not be fully up to date in their security measures. These organizations are also a critical link in their economies and are thus pressured to pay ransoms. Colleges and universities, especially those that are vulnerable through legacy systems and low security investments, could be next on the global hacker target list.

Figure 3: Major Known Data Breaches[9]



Source: Bloomberg, 2019

Our devices, systems, and networks are constantly under threat of a cyberattack. Typical cyberthreats include social engineering, distributed denial of service (DDoS), botnets, and malware. Social engineering is the use of deception to manipulate individuals into exposing information that will be used for fraudulent purposes. DDoS cyberattacks render a website or server inoperable, normally by overloading it with traffic from botnets. Botnets are a network of infected computers that are remotely controlled by a cybercriminal.[10] On October 21st, 2016 the Mirai botnet lead a massive DDoS attack that rendered high-profile websites, such as Netflix,

[8] https://digitalguardian.com/blog/what-cyber-security

[9] https://www.bloomberg.com/graphics/corporate-hacks-cyber-attacks/

[10] https://usa.kaspersky.com/resource-center/threats

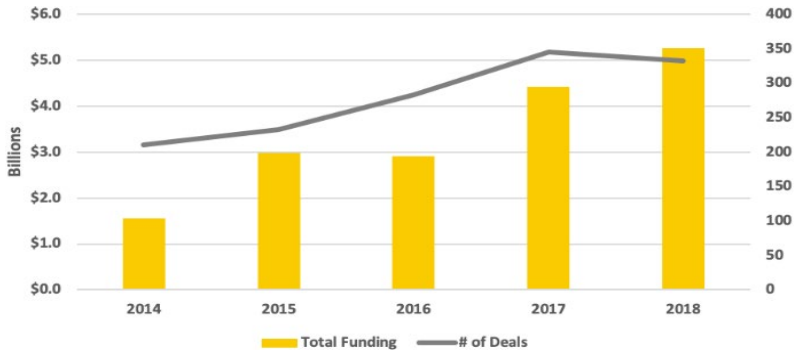
Twitter, and Airbnb, inoperable for users on the U.S. east coast. This cyberattack exploited weaknesses within the internet of things (IoT), which are everyday devices that are connected to the internet, to infect 600,000 devices.[11]

Highlights of U.S. and Global Cybersecurity Industry

Worldwide spending on information security products and services reached more than $114 billion in 2018, up 12.4% from 2017. A survey conducted by Gartner revealed that the three top drivers of cybersecurity spending are security risks, business needs, and industry changes. Privacy was another top concern that has become more prevalent as compared to past surveys.[12]

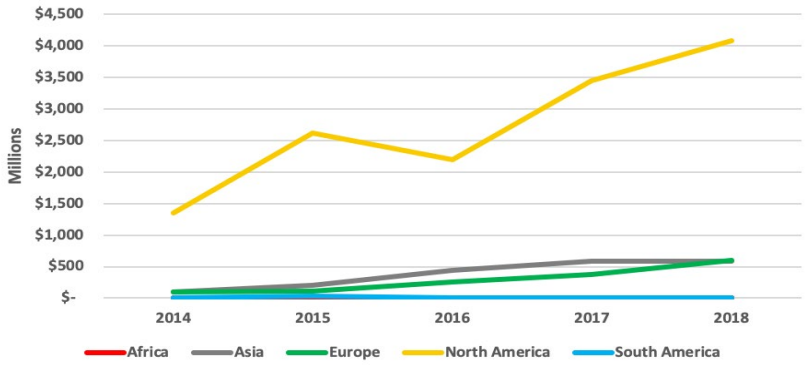
Venture capital firms invested $5.3 billion into cybersecurity companies globally in 2018, with over $4 billion being invested in North America. While the total number of deals did not grow from 2017 to 2018, the aggregate value of the deals increased by 20%. Notable initial public offerings (IPOs) for the year raised $1.4 billion among four firms, Avast Software, Tenable, Zscaler, and Carbon Black.[13]

Figure 4: Global Cybersecurity VC Investment



Source: Strategic Cyber Ventures, 2018

Figure 5: Cybersecurity VC Investment by Region



Source: Strategic Cyber Ventures, 2018

[11] https://www.whiteops.com/blog/9-of-the-most-notable-botnets

[12] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[13] https://scvgroup.net/2018-cybersecurity-venture-capital-investment/

The White House has deemed cybercrime to be one of the biggest issues facing national security and proposed a 5% increase in cybersecurity spending for the FY 2020 President's Budget. The total amount budgeted is $17.4 billion, with $9.6 billion being allocated to the Department of Defense.[14]

Organizations are spending more money to combat cybercrime, as the average cost per organization grew 62.5% from 2013 to 2017.[15] The costs will continue to rise as cyberattacks increase in frequency and sophistication. For example, by the end of 2019, ransomware is expected to attack an organization every 14 seconds and bring $11.5 billion in damages for the year. This is a significant increase compared to ransomware attacks in 2015, which were estimated to have caused $325 million in damages, occurring every 2 minutes.[16]

The high demand for cybersecurity professionals has caused organizations to compete for talent. Research by the International Information System Security Certification Consortium found that 38% of cybersecurity professionals who are actively seeking employment are contacted multiple times per day by recruiters. It was also found that 48% of all cybersecurity professionals are contacted weekly, whether or not they are actively looking for employment.[17]

The importance of cybersecurity cannot be ignored. The domestic and global trends toward growing investment and spending on cybersecurity demonstrates that organizations understand constructing a strong cybersecurity program is vital to their survival. Companies and governments wanting to succeed in the digital world have created an increased need for cybersecurity professionals. Demand for skilled professionals in the industry is soaring, and there is not enough qualified talent to satisfy that demand. The deficit is expected to increase in the future. U.S. higher education institutions should consider preparing students and professionals for current and future jobs within cybersecurity.

[14] https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf

[15] https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[16] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[17] https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx

Trends in Cybersecurity

A few of the most important trends in cybersecurity include advances in social engineering, increasing governmental regulation of data gathering and use, vulnerabilities of the internet of things, the professional talent gap, and the evolution of educational programs.

Spear Phishing Gets More Personal

Spear phishing is one of the most common types of social engineering. Amateur phishing schemes are becoming a thing of the past as perpetrators can now launch localized and personalized attacks on unsuspecting victims using emails, instant messaging, SMS, and social media. The use of forged sender addresses and spoofed identities allow attackers to appear to be a legitimate source. Messages contain either malicious file attachments or embedded links to direct users to an untrustworthy source.[18] A study by Trend Micro found that over 90% of cyberattacks began with a spear phishing email. The study found that 94% of these emails used malicious file attachments while 6% used links to gain unauthorized access or cause damages.[19]

Increased Regulation on Data and Consumer Privacy

The European Union is the First to Enact Sweeping Data Protection Laws

The European Union implemented legislation known as General Data Protection Regulation (GDPR) in mid-2018. This policy aims to give individuals control over their personal data and to unify data regulation across the European Union. Businesses that handle personal data are required to provide data safeguards, such as encryptions, and must provide individuals with the highest possible privacy setting by default. Data cannot be made available publicly without explicit, informed consent from an individual, and they may revoke their consent at any time. Data cannot be used to identify individuals without additional information, which is required to be stored separately as an added precaution. Any business that revolves around personal data processing is required to appoint a Data Protection Officer (DPO). If a business experiences a data breach that adversely affects user privacy, they must report the incident within 72 hours. For severe violations, fines could be 20 million euros or up to 4% of the violator's total global turnover of the preceding fiscal year, whichever is higher.[20]

Data Protection in the United States

Overarching data protection legislation does not exist in the U.S. Instead, there are federal and state laws that relate to various forms of data protection. Regulation at the federal level provides standards for federal agencies, financial institutions, and healthcare organizations. These pieces of legislation include the 1996 Health Insurance Portability and Accountability Act (HIPAA), 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act.[21]

---

[18] https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref

[19] https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email

[20] https://gdpr-info.eu

[21] https://www.appknox.com/blog/united-states-cyber-security-laws

Vulnerabilities of the Internet of Things

Current IoT Flaws

As a broader range of devices become equipped to connect to the Internet, it becomes easier for cybercriminals to bypass network security by targeting the endpoint device with the weakest security.[22] The internet of things (IoT) has expanded to include devices such as coffee makers, lights, thermostats, ovens, laundry machines, and yoga mats, which creates more potential vulnerabilities. One of the most significant IoT vulnerabilities is that owners rarely change the factory default usernames and passwords, which can be found online, in catalogs, or by purchasing the same device. Similarly, there is often a lag between the time when critical software patches are released and when they are downloaded by device owners, allowing cybercriminals time to continue exploiting glitches and faulty programming for weeks or months after the problem has been made public and corrected by the device manufacturer.[23]

Problems with IoT Device Manufacturers

Manufacturers generally do not prioritize product security for various reasons. First, it hinders bringing as many devices to the market as cheaply and quickly as possible. Second, they are not required by regulation, in the U.S., to perform security checks on their devices, which are also expensive and time-consuming. Third, embedding an adequate level of security into IoT devices may require expertise that the manufacturer does not have and could involve product redesigns to accommodate different processors needed to operate the upgraded security. [24] The combination of these shortsighted decisions makes IoT devices easy for hackers to exploit. A survey from strategy consulting firm Altman Vilandrie & Company found that 48% of U.S. companies with IoT devices on their network have been breached at least once.[25]

Cybersecurity Talent Gap

Careers in Cybersecurity

The combination of continuous advancements in technology, increases in cybersecurity threats, and regulatory changes have all led to strong demand for cybersecurity professionals. These factors additionally provide a reason for organizations to invest in their existing staff. In 2017, 40% of security professionals said breaches are driving increased investment in the training of security staff, compared with 37% in 2016.[26] Cybersecurity professionals are needed across industries, in both the public and private sectors, to protect organizations from malicious threats.[27] Most affected by potential cybersecurity staffing shortages are the educational, financial, governmental, healthcare, manufacturing, online retail, and transportation

[22] https://www.csoonline.com/article/3241242/cybersecurity-trends-to-watch.html

[23] https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html

[24] https://www.aberdeen.com/techpro-essentials/iot-device-security-seriously-neglected/

[25] https://www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security

[26] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

[27] https://www.redteamsecure.com/the-top-6-industries-at-risk-for-cyber-attacks/

industries.[28] Projections by Cisco point to a global shortage of two million cybersecurity professionals by the end of 2019.[29]

Effects of the Talent Gap

One immediate ramification of the talent shortage is that 54% of companies are working with external security consultants, and 47% are outsourcing incident response. Outsourcing these security services allows existing employees to focus on strategic initiatives, rather than spending all their time reacting to problems.[30] A second effect of the talent gap is that companies may lack depth among their cybersecurity professionals. Cybersecurity encompasses a broad range of technical skills and organizations facing talent gaps will have weaknesses in their security protocols. Lastly, employers are not sure how to identify qualified applicants.[31] The field is not fully established yet, and employers struggle to clearly define job qualifications and responsibilities.[32]

Cybersecurity Degrees vs. Certifications

Cybersecurity Education Changes as Cybersecurity Evolves

There are several different aspects of cybersecurity, with industry professionals holding one or more areas of specialization, in addition to their general IT knowledge. Since cybersecurity is ever-changing in response to threats and technological advances, professionals must keep their skills current in order to stay competitive. Relevant university degrees provide a strong foundation, upon which individuals can build specific skills. Top areas of knowledge sought-after by employers in cyber security encompass the following:

Top Knowledge Areas Requested of Cybersecurity Professionals

-Information Security
-Information Systems
-Network Security
-Information Assurance
-Vulnerability Assessment
-Project Management
-Computer Forensics
-Auditing
-Risk Assessment
-Security Operations
-Penetration Testing
-Authentication[33]

[28] https://www.globalsign.com/en/blog/top-industries-preparing-for-evolving-cybersecurity-threats/

[29] https://gblogs.cisco.com/ch-tech/closing-the-cyber-security-talent-gap/Trends

[30] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

[31] https://www.secureworldexpo.com/industry-news/impacts-of-cybersecurity-talent-shortage-gap

[32] https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx

[33] https://www.cyberseek.org/pathway.html

University Cybersecurity Curriculums

As the demand for professionals to work within cybersecurity continues to increase, so does the pressure on higher education institutions to prepare their students. Universities are creating degree programs from within their existing computer science, business, and engineering departments while simultaneously developing new information technology courses in response to real world needs. Common courses include the following:

Bachelor's Degree Course Curriculum

-Operating Systems
-Network Security
-Information Assurance
-Digital Forensics
-Computer Ethics and Privacy
-Object-Oriented Programming
-Project Management

Graduate Degree Course Curriculum

-Computer Forensics
-Cyber Law
-Introduction to Data Mining
-Telecommunication Systems
-Secure Software Design
-Risk Analysis[34]

Professional Education

University degrees tend to lack specialized technical skills. Currently, there are several certifications that can validate specialized or generic skillsets within cybersecurity. Certifications help individuals advance their career and make it easier for companies to identify workers to fill their cybersecurity needs.

Top Certifications Requested by Employers

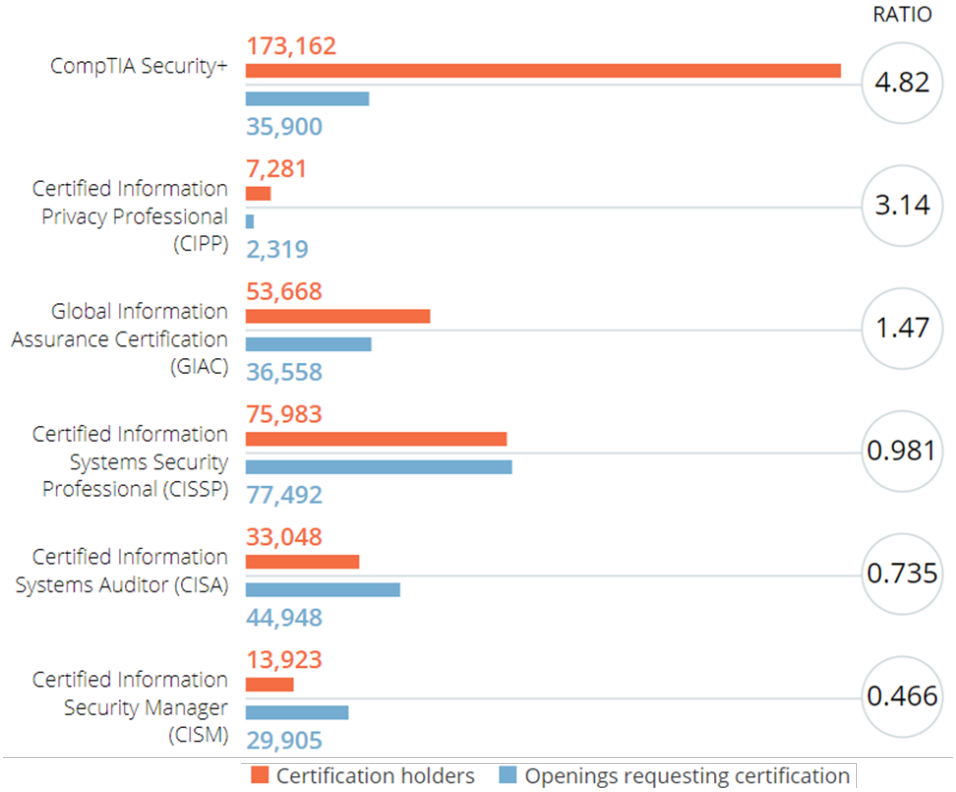
-Certified Information System Auditor (CISA)
-Certified Information Security Manager (CISM)
-Certified Information Privacy Professional (CIPP)
-Certified Information Systems Security Professional (CISSP)
-CompTIA Security+
-Certified Ethical Hacker (CEH)
-Cisco Certified Network Associate
-GIAC Certifications
-Microsoft Certified Systems Engineer[35]

[34] https://www.cybersecurityeducation.org/courses/

[35] EMSI Job Posting Analytics, 2019

The most popular professional designations include CISA, CISM, CISSP, GIAC, and Security+. The Security+ certificate is held by 173,162 professionals, CISSP by 75,983, and GIAC by 53,668. In job postings, the certification that is requested most often is CISSP.[36]

Figure 6: Certification Holders vs. Openings Requesting Certification



Source: CyberSeek, 2019

[36] https://cyberseek.org

Occupational Analysis

Current Available Jobs Related to Cybersecurity

For the purpose of this research, six cybersecurity-related occupation were selected: information security analysts; network and computer systems administrators; computer and information systems managers; software developers: application software developers: systems software; and computer systems analysts. While these are not the only occupations that use, or would benefit from, cybersecurity expertise, they provide valuable insight into the overall market while demonstrating potential career paths for professionals.

Occupational and job analysis in this research is focused on two areas: the U.S., broadly, and on a specific company, Oracle Corporation, which is used as an example. While this research is not exhaustive, its purpose is to provide a sense of the current need for professionals in the industry.

This report presents occupational and demographic information for cybersecurity-related jobs on a national level. Also included, is the employment outlook for emerging jobs that will require cybersecurity knowledge. Unless stated otherwise, all figures and tables are taken directly from Economic Modeling Specialists International (Emsi) and its 2019.3 datasets.

Region: United States

Table 1 outlines the current and forecasted occupational data for select cybersecurity occupations in the United States. Over the next 10 years, these occupations are forecasted to see 15% growth, with software developers (24%) and information security analysts (22%) each forecasted to experience over 20% growth. Three of the six highlighted occupations have median annual earnings above $100,000. All of the occupations typically require a bachelor's degree for entry-level positions.

Table 1: Current and Forecasted Occupational Data for Select Cybersecurity Occupations

Occupation	Total Jobs		2019 - 2029 Change		Annual Openings	Median Annual Earnings	Typical Entry Level Education
	2019	2029	# Change	% Change			
Software Developers, Applications	1,037,235	1,286,872	249,637	24%	98,717	$102,578	Bachelor's Degree
Computer Systems Analysts	687,721	748,070	60,349	9%	51,875	$87,904	Bachelor's Degree
Computer and Information Systems Managers	455,149	510,815	55,666	12%	40,607	$139,113	Bachelor's Degree
Software Developers, Systems Software	455,061	499,992	44,931	10%	35,072	$108,981	Bachelor's Degree
Network and Computer Systems Administrators	398,365	424,125	25,760	6%	28,190	$81,315	Bachelor's Degree
Information Security Analysts	120,073	146,531	26,458	22%	11,516	$98,326	Bachelor's Degree
Total/Average	**3,153,603**	**3,616,404**	**462,801**	**15%**	**265,978**	**$100,651**	

Figure 7 shows the number of jobs, their predicted growth, and average hourly earnings for select cybersecurity professionals in the United States. There are over three million jobs for these occupations, and they are forecasted to experience strong growth of 14.7% by 2029. The average hourly rate for related professionals is currently $48.39, or $100,651 annually, which is consistent with the average median salary on Table 1.

Figure 7: Occupation Overview for Select Cybersecurity Occupations

3.15M	+14.7%	$48.39/hr
Jobs (2019)	⊞ % Change (2019-2029)	⊞ Median Hourly Earnings

Map 1 shows jobs across the U.S. for select cybersecurity occupations in 2019. The top states include California (475,928 jobs), Texas (255,632), New York (199,027), Virginia (153,434), and Florida (143,846).

Map 1: Concentration of Select Cybersecurity Occupations by State

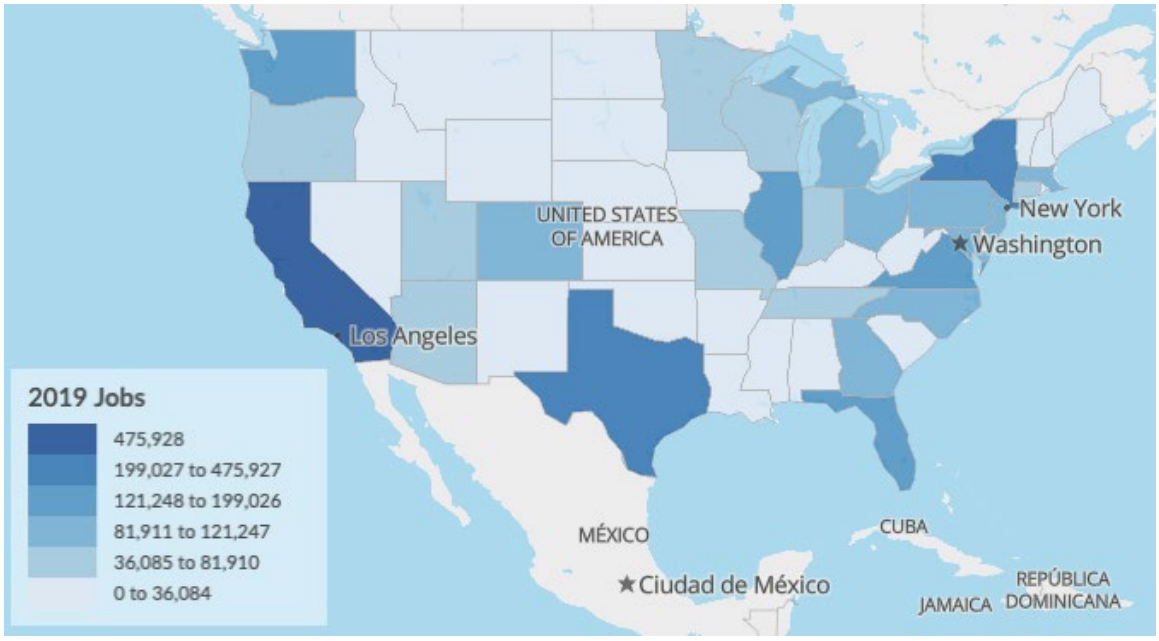


Figure 8, below, highlights the number of job postings for select cybersecurity across the United States for the 12 months ending June 2018. Out of 17.26 million job postings, 3.22 million were unique, resulting in a posting intensity of 5:1, which is higher than the national average for all occupations. This suggests that cybersecurity professionals are in greater demand compared to the average occupation.

Figure 8: Job Postings for Select Cybersecurity Occupations

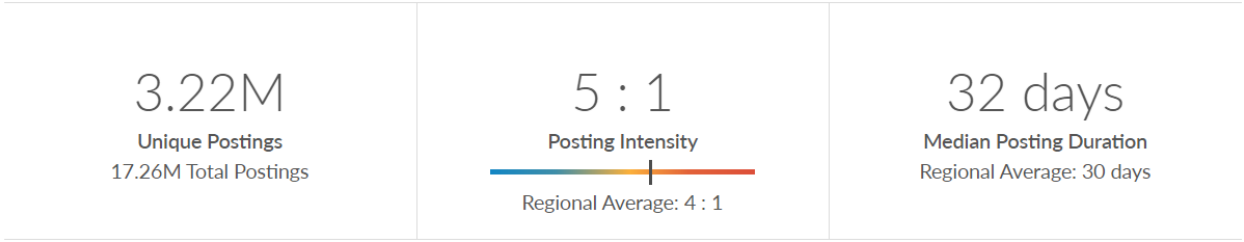


Figure 9 details the types of degrees professionals in the field hold. In 2017, computer and information sciences, general was most popular (42,710) with computer science closely behind with (41,529). The top five degrees show that most professionals in cybersecurity have an educational background relating to information technology.

Figure 9: Degree Types for Select Cybersecurity Occupations

CIP Code	Program	Completions (2017)
11.0101	Computer and Information Sciences, General	42,710
11.0701	Computer Science	41,529
11.0103	Information Technology	22,645
11.0401	Information Science/Studies	16,615
11.0901	Computer Systems Networking and Telecommunications	13,574

Figure 10 lists the industries in which these professionals are employed. Computer systems design services (435,893) and custom computer programming services (417,210) lead the list by a significant margin.

Figure 10: Industries Hiring for Select Cybersecurity Occupations

Industry	Occupation Group Jobs in Industry (2018)	% of Occupation Group in Industry (2018)	% of Total Jobs in Industry (2018)
Computer Systems Design Services	435,893	14.2%	37.0%
Custom Computer Programming Services	417,210	13.6%	36.7%
Corporate, Subsidiary, and Regional Managing Offices	185,816	6.1%	7.0%
Software Publishers	168,823	5.5%	36.3%
Data Processing, Hosting, and Related Services	89,618	2.9%	21.5%

Currently Emerging Jobs Related to Cybersecurity

Figure 11 highlights the number of national job postings across all occupations that include the keywords "cybersecurity," "cyber security," or "information security." Out of 3.60 million job postings, 611,766 were unique, resulting in a posting intensity of 6:1, suggesting that organizations are actively trying to fill these positions.

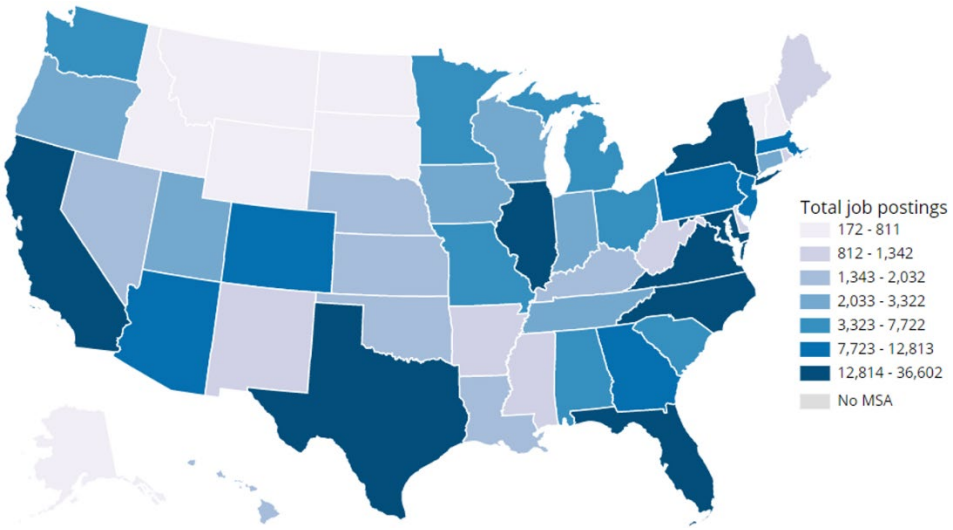
Figure 11: Job Postings that Containing Keywords Across All Occupations

611,766	6 : 1	37 days
Unique Postings	Posting Intensity	Median Posting Duration
3.60M Total Postings	Regional Average: 4 : 1	Regional Average: 30 days

Supply and Demand

Another metric for examining the talent gap in the U.S. is the ratio of existing cybersecurity workers to cybersecurity job openings. A low ratio could come from having too few workers (low supply), excessive job postings (high demand), or a combination of both. According to CyberSeek, the national average for all jobs is 5.8 while the national average for cybersecurity jobs is only 2.3, with Washington D.C. having the lowest ratio of 1.4. For the 12 months ending August 2018, there were an estimated 715,715 employed cybersecurity workers and 313,735 job openings. California is the state with the most openings by having more than 36,000 job postings.[37]

Map 2: Cybersecurity Job Postings by State



Source: CyberSeek, 2019

[37] https://www.cyberseek.org/heatmap.html

Job Titles

Various reports and job posting sites were examined to determine existing and emerging jobs within cybersecurity. The following job titles were mentioned:

-Cybersecurity Specialist / Technician
-Cybercrime Analyst / Investigator
-IT Auditor
-Incident Analyst / Responder
-Cybersecurity Analyst
-Cybersecurity Consultant
-Penetration and Vulnerability Tester
-Cybersecurity Manager / Administrator
-Cybersecurity Engineer
-Cybersecurity Architect[38]

Salary Expectations

According to the Bureau of Labor Statistics, the median annual wages across all computer occupations was $86,320 in May 2018[39] while more specialized technology workers such as information security analysts earn an average median salary of $98,322. The metro areas in the U.S. with the highest average salaries for cybersecurity professionals include Silicon Valley, New York City, District of Columbia, and Boston. Technology companies, occupations, and professionals are heavily concentrated in these locations, attributing to the higher pay.[40]

Education & Skill Requirements

Skillsets across cybersecurity professionals can vary greatly depending on the type of work requested by an employer. However, there are several skills that satisfy the qualifications for most jobs in the industry. Although requirements vary among jobs, almost all require a bachelor's degree in computer science or a related field. Additionally, certifications are commonly required, especially for specialized or senior level positions. These skills are often required:

-C++, Java, Python, PHP, Perl, Shell
-Current understanding of common web vulnerabilities
-Knowledge and awareness of industry standards, practices, procedures, and methods
-Operating system architecture, administration, and management knowledge[41]
-Threat modeling, vulnerability assessment, penetration testing, intrusion detecting
-Risk analysis and mitigation
-Cloud security[42]
-Digital forensics
-Security incident handling and response
-Audit and compliance[43]

[38] https://cyberseek.org

[39] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-5

[40] https://insights.dice.com/2018/07/11/cyber-security-salary-titles-skills/

[41] https://insights.dice.com/cybersecurity-skills/

[42] http://techgenix.com/cybersecurity-skills/

[43] http://blog.cipher.com/the-must-have-skill-sets-certifications-for-cyber-security-careers

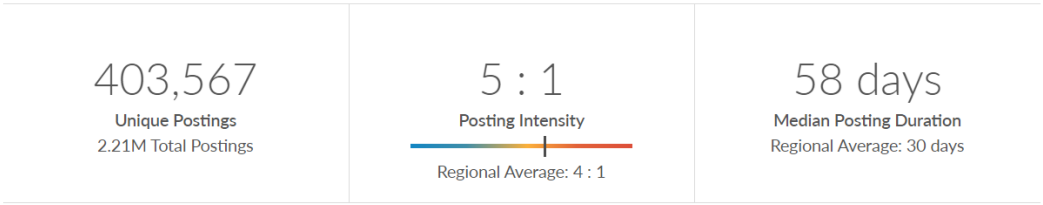
Job Posting Analytics of Example Firm: Oracle Corporation

Oracle is a computer technology company offering enterprise software, cloud engineered systems, and database hardware and software. Not only does the firm hire many of the jobs previously mentioned, but it also hires product managers, sales representatives, and cloud engineer architects. Oracle is highlighted as an example of the impact cybersecurity has on various job markets, since the firm is a leader in computer technology and is constantly adapting to industry trends.

All figures and tables in this section are taken directly from Economic Modeling Specialists International (Emsi) and its 2019.3 datasets.

Figure 12 shows that Oracle had 2.21 million total job postings, of which 403,567 were unique, resulting in a 5:1 job posting intensity. The median post duration, 58 days, was almost twice that of the national average.

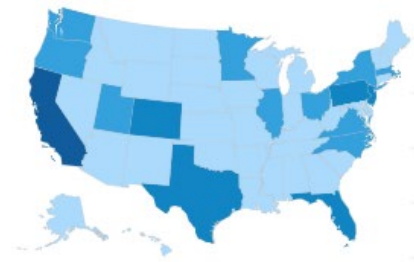
Figure 12: Job Postings Overview for Oracle Corporation



Source: Economic Modeling Specialists International (EMSI) 2019.3 Dataset

Figure 13 demonstrates the geographic breakdown of these job postings. The highest concentration by far is found for positions located in California (75,062 postings), followed by Florida (22,907) and New Jersey (22,889). Oracle is headquartered in Redwood City, California and has 11 other offices in the state all of which contribute to the large volume of job postings in California.

Figure 13: Regional Breakdown of Job Postings for Oracle Corporation



State	Unique Postings (Jul 2018 - Jun 2019)
California	75,062
Florida	22,907
New Jersey	22,889
Pennsylvania	22,386
Colorado	22,192

Source: Economic Modeling Specialists International (EMSI) 2019.3 Dataset

Figure 14 outlines the cities in which these jobs are located. The top two cities are Seattle and Redwood City. Corresponding with Figure 13, four of the top cities are in California and have a combined 18,505 unique postings for the time period.

Figure 14: Top Posted Cities for Oracle Corporation

City	Total/Unique (Jul 2018 - Jun 2019)	Posting Intensity	Median Posting Duration
Seattle, WA	60,976 / 7,130	9 : 1	52 days
Redwood City, CA	32,107 / 5,776	6 : 1	53 days
Sacramento, CA	27,457 / 4,518	6 : 1	59 days
Troy, MI	33,437 / 4,361	8 : 1	59 days
Austin, TX	42,403 / 4,357	10 : 1	57 days
San Francisco, CA	26,991 / 4,351	6 : 1	53 days
Washington, DC	23,567 / 4,068	6 : 1	55 days
Tucson, AZ	23,451 / 3,870	6 : 1	64 days
San Jose, CA	21,975 / 3,860	6 : 1	55 days
San Antonio, TX	30,126 / 3,829	8 : 1	61 days

Source: Economic Modeling Specialists International (EMSI) 2019.3 Dataset

Figure 15 displays the top occupations posted by Oracle in 2018. Software developers, applications were first in the total number of job postings.

Figure 15: Top Posted Occupations for Oracle Corporation

Occupation (SOC)	Total/Unique (Jul 2018 - Jun 2019)	Posting Intensity	Median Posting Duration
Software Developers, Applications	232,955 / 49,077	5 : 1	66 days
Marketing Managers	182,912 / 44,110	4 : 1	50 days
Sales Representatives, Wholesale and Manufacturing, Technical and Scientific Products	426,453 / 39,789	11 : 1	60 days
Computer Occupations, All Other	174,727 / 38,828	5 : 1	65 days
Sales Managers	178,932 / 29,683	6 : 1	62 days
Computer and Information Systems Managers	73,238 / 17,318	4 : 1	56 days
Sales Engineers	121,245 / 16,111	8 : 1	60 days
Sales Representatives, Services, All Other	108,763 / 15,528	7 : 1	55 days
Management Analysts	60,690 / 12,398	5 : 1	58 days
Computer Systems Analysts	52,284 / 11,196	5 : 1	55 days

Source: Economic Modeling Specialists International (EMSI) 2019.3 Dataset

Figure 16 shows which job titles Oracle posted most frequently. Sales representatives had the highest number of unique job postings at 21,581, followed by software engineers with 18,083.

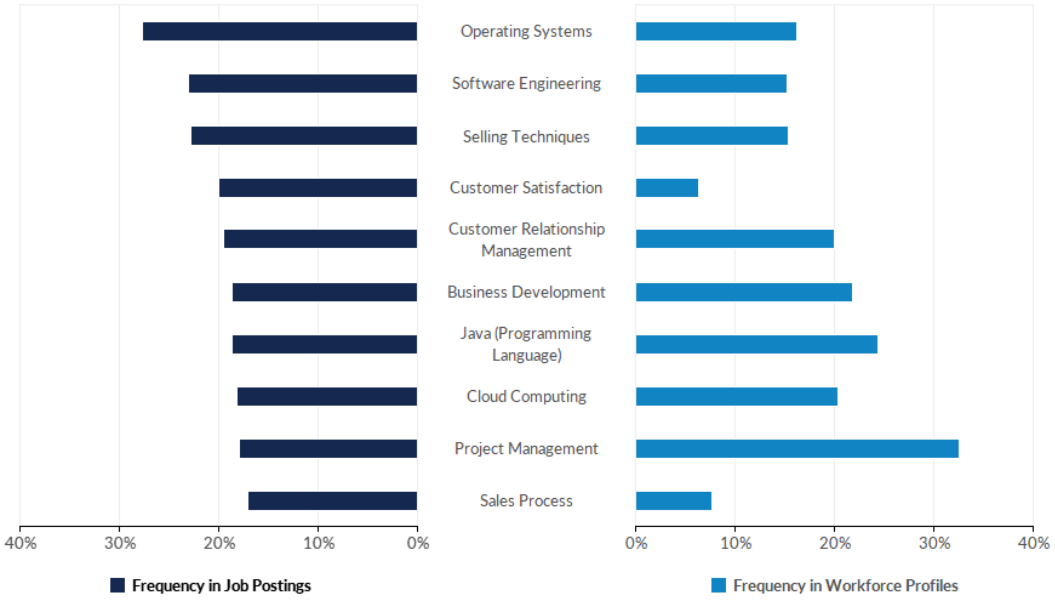
Figure 16: Top Posted Job Titles for Oracle Corporation

Job Title	Total/Unique (Jul 2018 - Jun 2019)	Posting Intensity	Median Posting Duration
Sales Representatives	282,287 / 21,581	13 : 1	62 days
Software Engineers	97,091 / 18,083	5 : 1	67 days
Product Managers (Management)	67,474 / 16,717	4 : 1	57 days
Sales Managers (Management)	111,359 / 13,990	8 : 1	63 days
Cloud Engineer Architects	52,814 / 12,561	4 : 1	59 days
Project Managers (Computer and Mathematical)	33,420 / 7,465	4 : 1	54 days
Technical Sales Representatives	66,711 / 7,174	9 : 1	60 days
Marketing Managers (Management)	22,204 / 7,021	3 : 1	51 days
Project Managers (Management)	29,238 / 5,813	5 : 1	55 days
Consulting Directors	27,105 / 5,267	5 : 1	68 days

Source: Economic Modeling Specialists International (EMSI) 2019.3 Dataset

Figure 17 charts the most frequently posted hard skills listed in each job posting by Oracle. The most common were knowledge of operating systems (28%), software engineering (23%), and selling techniques (23%).

Figure 17: Top Posted Hard Skills for Oracle Corporation



Source: Economic Modeling Specialists International (EMSI)

Figure 18 shows a breakdown of the most frequently posted common skills listed in each job posting by Oracle. Management is the most popular common skill listed, appearing in 73% of postings. Sales appears in 36% of job postings, leadership in 40%, and communications in 38%.

Figure 18: Top Posted Common Skills for Oracle Corporation

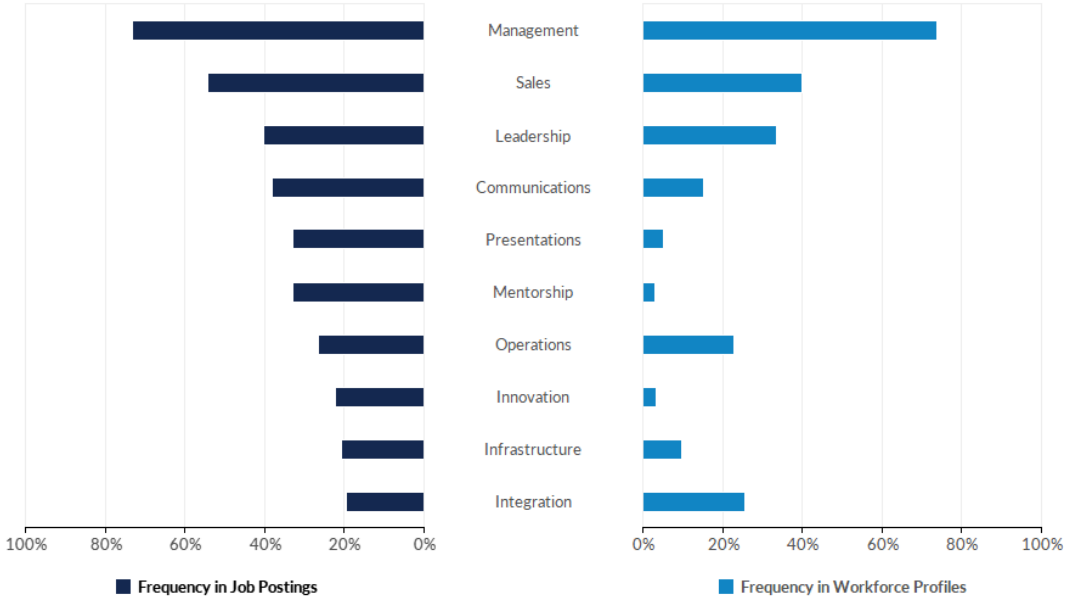


Figure 19 displays the monthly active postings for Blockchain, Inc. from September 2016 to June 2019. There is a clear growth trend, with a peak in March 2019 of 114,048 active postings.

Figure 14: Monthly Active Postings for Oracle Corporation

Source: Economic Modeling Specialists International (EMSI) 2019.3 Dataset

Impact on Higher Education

- Higher education has a great opportunity to be part of the cybersecurity professional supply solution, as they did by educating hundreds of thousands of computer scientists and technology workers over the decades. While some institutions claim that technology changes too quickly, others have stepped forward to address technology education and training needs. Many of these institutions are community colleges and private industry. However, investing in the re-training and development of the workforce is what professional, continuing and online (PCO) units are supposed to be good at. In fact, unless the market and higher education responds, it is estimated that 3.5 million cybersecurity jobs will go unfilled by 2021.

- Investing in development of technology curriculum, while potentially costly and with a shorter lifespan than a degree, places the institution at the forefront of change. When attracting faculty and content experts, it also better connects the institution with the industry regarding cybersecurity and other technology issues and advancements. Institutions such as Georgia Tech, Johns Hopkins University, Harvard University, Kennesaw State University, Wake Forest University and others are offering degrees, certificates, or workshops in a variety of topics or specialties.

- The role of cybersecurity professional is not going away like the position of "webmaster" did. Demand for cybersecurity education and training will exist until the threat has been eliminated. To eliminate the threat, cybersecurity systems and data security processes will need to evolve at a faster rate than hackers can introduce new methods of cyber-attack. Until then, or until advances in artificial intelligence outpace and anticipate attacks, there should be opportunities for cybersecurity education and training.

- For the PCO unit, the potential revenue and lifecycle for cybersecurity education and training could be significant depending on competitive factors. Currently, media sources show an increase in ransom demands and security breaches. This would suggest that demand for training should be there. Given the relative "newness" of the Internet and mobile systems, we believe that society is at the beginning of the technological revolution and with it, more opportunities to better protect our systems.

- In addition to what appears to be a long lifespan for cybersecurity education and training, there are many depths or levels of training needed. Executive education opportunities exist where senior leaders need to understand the vulnerabilities and strategies that are needed to create a more secure corporate culture. Technology and information officers will need high level training. Managers will need to know how to implement technology and strength processes. All employees will need to understand safe practices and basics to prevent cyberattacks.

- If a PCO unit cannot respond fast enough, opportunities to partner with outside content experts exist. The UPCEA corporate community offers many options including certificate programs from HackerU and Trilogy. Partnering with a content company allows for colleges and universities to be part of the solution in their communities, as well as create revenue streams for PCO. Some partners, such as HackerU, also offer partner institutions' employees discounted prices for enrollment. Having a new training resource for the college or university could be an added benefit as the institution shores up its defenses by adding more knowledgeable cyber-professionals. An outsource relationship also puts the responsibility of keeping resources current with the outside provider.

Appendix

Cybersecurity Certifications

The Certified Information Systems Auditor (CISA) designation is issued by the Information Systems Audit and Control Association (ISACA) and displays that the bearer has successfully completed the CISA exam, has five years of relevant experience, adheres to the Code of Professional Ethics, and participates in the Continuing Professional Education (CPE) program. CISA is a gold standard for cybersecurity professionals who audit, control, monitor, and assess IT systems.[44] ISACA offers a separate certification for IT security and risk managers known as Certified Information Security Manager (CISM). CISM is an intermediate standard for information security management and the requirements for obtaining it include passing the CISM exam, having five years of relevant experience, following the Code of Professional Ethics, and participating in the CPE program.[45] Holders of either certification have the knowledge and skills to meet the dynamic challenges that organizations face.

The Certified Information Systems Security Professional (CISSP) certification is granted by the International Information System Security Certification Consortium (ISC)² for professionals in information security. Requirements include having five years of work experience as defined by the (ISC)[2] Common Body of Knowledge, passing the CISSP examination, obtaining an endorsement from a current credential holder, and adhering to the (ISC)[2] Code of Ethics. Earning the CISSP demonstrates that the holder has the skillset to effectively design, implement, and manage a cybersecurity program.[46]

Global Information Assurance Certificate (GIAC) is an entity that provides over 30 information security certifications. Their certifications target specialized skills compared to taking a generic approach. The GIAC certification validates specific skills of security professionals and developers with standards established on industry benchmarks.[47] The last prominent designation, Security+, is issued by CompTIA and is a standard for entry-level information security knowledge on performing core functions. Professional experience is not required, but the certification does include an exam. Upon successfully passing the exam, credential holders are required to renew the certification by completing 50 continuing education credits every three years.[48]

The Certified Ethical Hacker (CEH) certification is issued by the EC-Council and requires passing the CEH exam and having two years of relevant experience or enrolling in a training course in lieu of experience. This certification is for penetration testers as well as any other cybersecurity professional that works with the integrity of a network's infrastructure. The CEH designation demonstrates knowledge on assessing information systems for vulnerabilities using the same methods as cybercriminals and fixing those vulnerabilities.[49]

---

[44] http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

[45] http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

[46] https://www.isc2.org/Certifications/CISSP#

[47] www.GIAC.org

[48] https://certification.comptia.org/certifications/security

[49] https://cert.eccouncil.org/certified-ethical-hacker.html