CYBER BRAIN
ACADEMY

1281 9th Ave. Unit 3408
San Diego, CA 92101
(619) 631-3003
learn@cyberbrainacademy.com
cyberbrainacademy.com

Commitment

Impact

Accessibility

CYBER BRAIN ACADEMY

THE CYBER SECURITY TRAINING
YOU DESERVE

www.cyberbrainacademy.com

About Us

TABLE OF CONTENTS

About Us

Cyber Brain Academy is a minority and veteran-owned small business headquartered in San Diego, California. We are an experienced IT training company that expertly prepares learners to attain industry-recognized IT certifications. Cyber Brain Academy delivers an effective cyber security education experience through our collaboration with academia, expert cyber security professionals, and our industry and vendor partnerships.

Mission Statement

Our goal is to deliver exceptional IT certification training to the cyber security workforce.

Vision Statement

Our company aspires to elevate security professionals through the power of education.

Chief Executive Officer – Mr. Victor Nzeata, MS, CEH, CISSP

Cyber Brain Academy is founded with service at its core. As a leader in military cyberspace operations, Mr. Victor Nzeata founded Cyber Brain Academy to support service members entering the cyber security workforce. He is recognized as the Army Reserve's first Cyber Operations Officer and has led multiple cyber operations within various countries. He has held roles such as electrical engineer, software engineer, cyber threat emulation lead, lead cyber security engineer and information systems security manager. Mr. Nzeata received his bachelor's degree in computer engineering technology from Purdue University, his master's degree in cyber security operations and leadership from the University of San Diego and is a Ph.D. candidate in information assurance and cyber security from Capella University.

In 2015, Mr. Nzeata successfully trained a peer group of 12 US Army Second Lieutenants to all pass the CISSP examination through an effective learning strategy. After this accomplishment, the vision for Cyber Brain Academy was created and he started to conceptualize what the company would entail. His vision manifested into Cyber Brain Academy, a certification training company that offers quality training at an affordable cost.

Chief Learning Officer – Ms. Natalie Scott, MA

Ms. Natalie Scott is an experienced education professional skilled in curriculum and instructional design. As the Chief Learning Officer of Cyber Brain Academy, she collaborates with experienced cyber security professionals and industry experts. She oversees the student learning experience and reports student engagement and performance to the CEO. Ms. Scott obtained her bachelor's degree in elementary education from Franklin College and her master's degree in curriculum and instruction from Ashford University. She has experience teaching and designing curriculum for students of all ages including elementary and higher education classes.

Ms. Scott joined the Cyber Brain Academy team in 2017 and has utilized her experience in the education field to enhance the curriculum and instruction components of both on-demand and instructor-led training. As Chief Learning Officer, she monitors student experience by providing surveys to evaluate both our curriculum and instructors, to ensure that we maintain the highest standard of quality.

Our Approach to Training

Cyber Brain Academy provides a comprehensive training experience by conducting our training in three phases – Pre-Training, Live-Online Training, and Post-Training – to ensure optimum success.

Phase 1: Pre-Training

Phase 1 consists of early access to your course materials. You will be given access to your course materials 14 days prior to your training experience. This allows for an engaging training experience and increased competency during Phase 2. All of our training materials are up to date and cover the latest version of each certification exam.

Phase 2: Five Day Live-Online, Instructor-led Training

Phase 2 consists of comprehensive instruction by our vendor-authorized instructor. Your five day live-online training session consists of engaging training materials, practice questions, daily recaps, and question & answer sessions between you and our experienced instructor.

Phase 3: Post-Training

Phase 3 consists of reviewing your gained competency through our provided course materials. Our team of certified instructors will be available one month after your course to answer any questions that you may have about your training experience. This is a feature only provided through Cyber Brain Academy and demonstrates our ongoing commitment to you.

Product Overview

Certified Information Systems Security Professional (CISSP) Live-Online Instructor-Led Training

This course entails five days of comprehensive instruction by an (ISC)^2 authorized CISSP instructor. The live-online training session consists of engaging training material, practice questions, daily-recaps, and question and answer sessions between you and our experienced instructor. Please refer to the training schedule for a detailed breakdown of course topics and activities.

Students will receive in-depth, technical CISSP domain knowledge that covers Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Included:

- An Expert (ISC)^2 Authorized CISSP Instructor
- Official (ISC)^2 CISSP Practice Tests
- Certificate of Completion – 40 Continuing Education Credits

Class Schedule:

	CISSP Domains	Topics Covered
Day 1	Introductions	● Introductions and review of exam objectives
	Security and Risk Management	● Confidentiality, integrity, and availability concepts ● Security governance principles ● Compliance ● Legal and Regulatory Issues ● Professional ethics ● Security policies, standards, procedures and guidelines ● Q&A

	Asset Security	● Information and asset classification ● Ownership (e.g., data owners, system owners) ● Protect privacy ● Appropriate retention ● Data security controls ● Handling requirements ● Q&A
Day 2	Security Engineering	● Recap ● Engineering processes using secure design principles ● Fundamental concepts of security models ● Security evaluation models ● Security capabilities of information systems ● Security architectures, designs and solution elements vulnerabilities ● Web-based systems vulnerabilities ● Mobile systems vulnerabilities ● Embedded devices and cyber-physical systems vulnerabilities ● Cryptography ● Site and facility design secure principles ● Physical security ● Q&A
Day 3	Communication and Network Security	● Recap ● Secure network architecture design ● Secure network components ● Secure communication channels ● Network attacks ● Q&A
	Identity and Access Management	● Physical and logical assets control ● Identification and authentication of people and devices ● Identity as a service (e.g., cloud identity) ● Third-party identity services (e.g., on-premise) ● Access control attacks ● Identity and access provisioning lifecycle ● Q&A
Day 4	Security Assessment and Testing	● Recap ● Assessment and test strategies ● Security process data (e.g., management and operational controls) ● Security control testing ● Test outputs (e.g., automated, manual) ● Security architecture vulnerabilities ● Q&A
	Security Operations	● Investigations support and requirements ● Logging and monitoring activities ● Provisioning of resources ● Foundational security operations concepts ● Resource protection techniques ● Incident management ● Preventative measures ● Patch and vulnerability management ● Change management processes ● Recovery strategies ● Disaster recovery processes and plans ● Business continuity planning and exercises ● Physical security ● Personnel safety concerns ● Q&A
Day 5	Software Development Security	● Recap ● Security in the software development lifecycle ● Development environment security controls ● Software security effectiveness ● Acquired software security impact ● Q&A

	Domain Review	• Review of all topics • Final Q&A

Security+ Live-Online Instructor-Led Training

This course entails five days of comprehensive instruction by a CompTIA authorized Security+ instructor. The live-online training session consists of engaging training material, practice questions, daily-recaps, and question and answer sessions between you and our experienced instructor. Please refer to the training schedule for a detailed breakdown of course topics and activities.

Students will receive in-depth, technical Security+ domain knowledge that covers Threats, Attacks, and Vulnerabilities, Technology and Tools, Architecture and Design, Identity and Access Management, Risk Management, and Cryptography and PKI.

Included:

- An Expert CompTIA Authorized Security+ Instructor
- Official CompTIA Security+ Review Guide
- Certificate of Completion – 40 Continuing Education Credits

Class Schedule:

	Security+ Domains	**Topics Covered**
Day 1	Introductions	• Introductions and review of exam objectives
	Threats, Attacks, and Vulnerabilities	• Given a scenario, analyze indicators of compromise and determine the type of malware • Compare and contrast types of attacks • Explain threat actor types and attributes • Explain penetration testing concepts • Explain vulnerability scanning concepts • Explain the impact associated with types of vulnerabilities • Q&A
Day 2	Technology and Tools	• Recap • Install and configure network components, both hardware and software-based, to support organizational security • Given a scenario, use appropriate software tools to assess the security posture of an organization • Given a scenario, troubleshoot common security issues. • Given a scenario, analyze and interpret output from security technologies • Given a scenario, deploy mobile device securely • Given a scenario, implement secure protocols • Q&A

Day 3	Architecture and Design	● Recap ● Explain use cases and purpose for frameworks, best practices and secure configuration guides ● Given a scenario, implement secure network architecture concepts ● Given a scenario, implement secure systems design ● Explain the importance of secure staging and deployment concepts ● Explain the security implications of embedded systems ● Summarize secure application development and deployment concepts ● Summarize cloud and virtualization concepts ● Explain how resilience and automation strategies reduce risk ● Explain the importance of physical security controls ● Q&A
Day 4	Identity and Access Management	● Recap ● Compare and contrast identity and access management concepts ● Given a scenario, install and configure identity and access services ● Given a scenario, implement identity and access management controls ● Given a scenario, differentiate common account management practices ● Q&A
	Risk Management	● Explain the importance of policies, plans and procedures related to organizational security. ● Summarize business impact analysis concepts. ● Explain risk management processes and concepts. ● Given a scenario, follow incident response procedures. ● Summarize basic concepts of forensics. ● Explain disaster recovery and continuity of operations concepts. ● Compare and contrast various types of controls. ● Given a scenario, carry out data security and privacy practices. ● Q&A
Day 5	Cryptography and PKI	● Recap ● Compare and contrast basic concepts of cryptography ● Explain cryptography algorithms and their basic characteristics. ● Given a scenario, install and configure wireless security settings. ● Given a scenario, implement public key infrastructure. ● Q&A
	Domain Review	● Review of all topics ● Final Q&A

Certified Cloud Security Professional (CCSP) Live-Online Instructor-Led Training

This course entails five days of comprehensive instruction by an (ISC)² authorized CCSP instructor. Your live-online training session consists of engaging training material, practice questions, daily-recaps, and question and answer sessions between you and our experienced instructor. Please refer to the training schedule for a detailed breakdown of course topics and activities.

Students will receive in-depth, technical CCSP domain knowledge that covers Architectural Concepts & Design Requirements, Cloud Data Security, Cloud Platform & Infrastructure Security, Cloud Application Security Operations, and Legal & Compliance.

Included:

- An Expert (ISC)² Authorized CCSP Instructor
- Official (ISC)² CCSP Practice Tests
- Certificate of Completion – 40 Continuing Education Credits

Class Schedule:

	CCSP Domains	Topics Covered
Day 1	Introductions	● Introductions and review of exam objectives
	Domain 1: Cloud Concepts, Architecture and Design	● Understand Cloud Computing Concepts ● Describe Cloud Reference Architecture ● Understand Security Concepts Relevant to Cloud Computing ● Understand Design Principles of Secure Cloud Computing ● Evaluate Cloud Service Providers ● Q&A
Day 2	Domain 2: Cloud Data Security	● Recap ● Describe Cloud Data Concepts ● Design and Implement Cloud Data Storage Architectures ● Design and Apply Data Security Technologies and Strategies ● Implement Data Discovery ● Implement Data Classification ● Design and Implement Information Rights Management (IRM) ● Plan and Implement Data Retention, Deletion and Archiving Policies ● Design and Implement Auditability, Traceability and Accountability of Data Events ● Q&A
Day 3	Domain 3: Cloud Platform and Infrastructure Security	● Recap ● Comprehend Cloud Infrastructure Components ● Design a Secure Data Center ● Analyze Risks Associated with Cloud Infrastructure ● Design and Plan Security Controls ● Plan Disaster Recovery (DR) and Business Continuity (BC) ● Q&A
	Domain 4: Cloud Application Security	● Recap ● Advocate Training and Awareness for Application Security ● Describe the Secure Software Development Life Cycle (SDLC) Process ● Apply the Secure Software Development Life Cycle (SDLC) ● Apply Cloud Software Assurance and Validation ● Use Verified Secure Software ● Comprehend the Specifics of Cloud Application Architecture ● Design Appropriate Identity and Access Management (IAM) Solutions ● Q&A
Day 4	Domain 5: Cloud Security Operations	● Recap ● Implement and Build Physical and Logical Infrastructure for Cloud Environment ● Operate Physical and Logical Infrastructure for Cloud Environment ● Manage Physical and Logical Infrastructure for Cloud Environment ● Implement Operational Controls and Standards ● Support Digital Forensics ● Manage Communication with Relevant Parties ● Manage Security Operations ● Q&A
Day 5	Domain 6: Legal, Risk and Compliance	● Recap ● Articulate Legal Requirements and Unique Risks within the Cloud Environment ● Understand Privacy Issues ● Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment ● Understand Implications of Cloud to Enterprise Risk Management ● Understand Outsourcing and Cloud Contract Design ● Q&A
	Content Review	● Review of all topics ● Review of exam breakdown ● Practice test ● Final Q&A

CompTIA Cybersecurity Analyst (CySA+) Live-Online Instructor-Led Training

This course entails five days of comprehensive training by a CompTIA authorized CySA+ instructor. Your live-online training session consists of engaging training materials, practice questions, daily-recaps, and question & answer sessions between you and our experienced instructor. Please refer to the training schedule for a detailed breakdown of course topics and activities.

Students will receive in-depth, technical CySA+ domain knowledge that covers Threat Management, Vulnerability Management, Cyber-Incident Response, and Security Architecture and Tool Sets.

Included:

- An Expert CompTIA Authorized CySA+ Instructor
- Official CompTIA CySA+ Review Guide
- Certificate of Completion – 40 Continuing Education Credits

Class Schedule:

	CySA+ Domains	Topics Covered
Day 1	Introductions	• Introductions and review of exam objectives
	Threat Management	• Apply environmental reconnaissance techniques using • appropriate tools and processes • Analyze the results of a network reconnaissance • Implement or recommend the appropriate response and countermeasure to a network-based threat • Explain the purpose of practices used to secure a corporate environment • Q&A
Day 2	Vulnerability Management	• Recap • Implement an information security vulnerability management process • Analyze the output resulting from a vulnerability scan • Compare and contrast common vulnerabilities found in an organization • Q&A
Day 3	Cyber-Incident Response	• Recap • Distinguish threat data or behavior to determine the impact of an incident • Prepare a toolkit and use appropriate forensics tools during an investigation • Explain the importance of communication during the incident response process • Analyze common symptoms to select the best course of action to support incident response • Summarize the incident recovery and post-incident response process • Q&A
Day 4	Security Assessment and Testing	• Recap • Explain the relationship between frameworks, common policies, controls, and procedures • Use data to recommend remediation of security issues related to identity and access management • Review security architecture and make recommendations to implement compensating controls • Use application security best practices while participating in the Software Development Life Cycle (SDLC) • Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies • Q&A

Day 5	Domain Review	• Review of all topics • Review of exam breakdown • Practice test • Final Q&A

Certified Authorization Professional (CAP) Live-Online Instructor-Led Training

This course entails five days of comprehensive instruction by an (ISC)² authorized CAP instructor. Your live-online training session consists of engaging training material, practice questions, daily-recaps, and question and answer sessions between you and our experienced instructor. Please refer to the training schedule for a detailed breakdown of course topics and activities.

Students will receive in-depth, technical CAP domain knowledge that covers the Risk Management Framework, Categorization of Information Systems, Selection of Security Controls, Security Control Implementation, Security Control Assessment, Information System Authorization, and Monitoring of Security Controls.

Included:

- An Expert (ISC)² Authorized CAP Instructor
- Certificate of Completion – 40 Continuing Education Credits

Class Schedule:

	CAP Domains	**Topics Covered**
Day 1	Introductions	• Introductions and review of exam objectives
	Risk Management Framework (RMF)	• Describe the RMF Describe and distinguish between the RMF steps • Identify roles and define responsibilities • Understand and describe how the RMF process relates to the organizational structure • Understand the relationship between the RMF and System Development Life Cycle (SDLC) • Understand legal, regulatory and other security requirements • Q&A
Day 2	Categorization of Information Systems Selection of Security Controls	• Recap • Categorize the system • Describe the information system (including the security authorization boundaries) • Register the system • Identify and document (inheritable) controls • Select, tailor and document security controls • Develop security control monitoring strategy • Review and approve security plan • Q&A
Day 3	Security Control Implementation Information System Authorization	• Recap • Prepare for security control assessment • Develop security control assessment plan • Assess security control effectiveness • Develop initial security assessment report (SAR) • Review interim SAR and perform initial remediation actions • Develop final SAR and optional addendum • Develop plan of action and milestones (POAM) • Assemble security authorization package • Determine risk • Determine the acceptability of risk • Obtain security authorization decision • Q&A
Day 4	Monitoring of Security Controls	• Recap • Determine security impact of changes to system and environment • Perform ongoing security control assessments (e.g., continuous monitoring, internal and external assessments)

		• Conduct ongoing remediation actions (resulting from incidents, vulnerability scans, audits, vendor updates, etc.) • Update key documentation (e.g., SP, SAR, POAM) • Perform periodic security status reporting • Perform ongoing risk determination and acceptance • Decommission and remove system • Q&A
Day 5	Domain Review	• Review of all topics • Review of exam breakdown • Practice test • Final Q&A

EC-Council Certified Ethical Hacker (CEH) Live-online Instructor-led Training

The Certified Ethical Hacker program is a trusted and respected ethical hacking training Program that any information security professional will need. CEH is used as a hiring standard and is a core sought-after certification by many of the Fortune 500 organizations, governments, cybersecurity practices, and a cyber staple in education across many of the most prominent degree programs in top Universities around the globe.

Included:

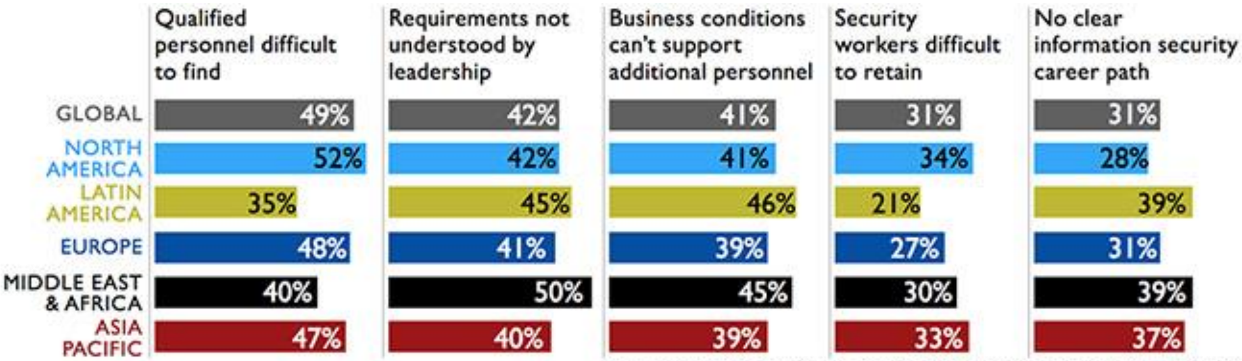
- An Expert EC-Council Authorized CEH Instructor
- Certified Ethical Hacker Official Study Guide
- Certificate of Completion – 40 Continuing Education Credits

Class Schedule:

	Topics Covered
Day 1	• Introductions and review of exam objectives • Introduction to Ethical Hacking • Footprinting and Reconnaissance • Scanning Networks • Enumeration • Vulnerability Analysis • Q&A
Day 2	• Recap • System Hacking • Malware Threats • Social Engineering • Sniffing • Denial-of-Service • Q&A
Day 3	• Recap • Session Hijacking • Evading IDS, Firewalls, and Honeypots • Hacking Web Servers • Hacking Web Applications • SQL Injection • Q&A
Day 4	• Recap • Hacking Wireless Networks • Hacking Mobile Platforms • IoT Hacking • Cloud Computing • Cryptography • Q&A
Day 5	• Review of all topics • Review of exam breakdown • Practice test • Final Q&A

Market Data: A Global Surplus of Over Two Million Cyber Security Roles

Inadequate staffing has been a prevalent issue for years. (ISC)² 2019 Cybersecurity Workforce Study estimates the shortage of needed skilled professionals is more than 4 million worldwide. This creates challenges for CISOs as they focus on protecting their organizations. - (ISC)² blog



Source: 2017 Global Information Security Workforce Study, (n = 12,709)

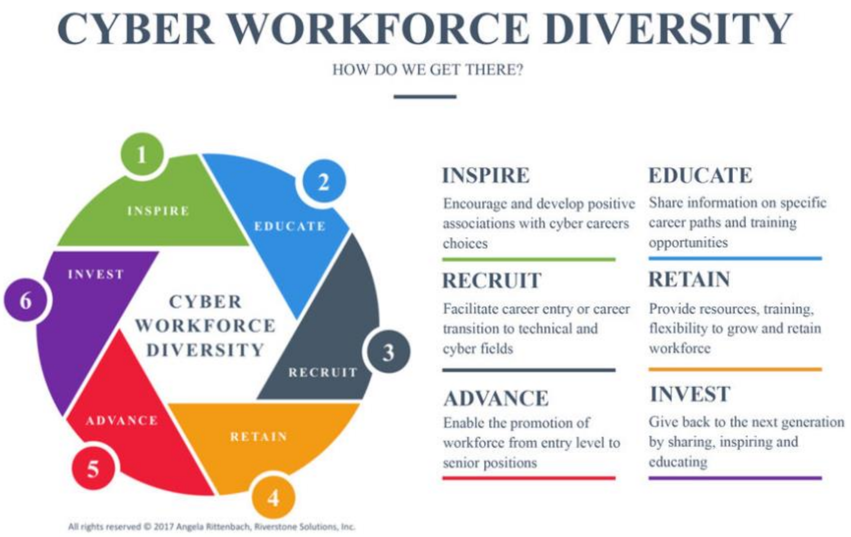
The global shortage of cyber security professionals is a national crisis. According to a recent survey conducted by (ISC)², "60% say their companies are at moderate or extreme risk of cybersecurity attacks due to this shortage." The global need for cyber security professionals can be attributed to the rise of cybercrime. In 2017, the WannaCry ransomware affected over 143 countries and caused over 4 billion dollars in fiscal losses. Businesses fall victim to ransomware attacks like WannaCry every 14 seconds. As cybercrime grows rampant, organizations are faced with a shortage of personnel to remedy internal security concerns.

- **By 2021, the global financial impact of cybercrimes will reach over 6 trillion dollars annually**

As well as an economic burden, the magnitude of cybercrimes can also have kinetic effects. To elaborate, in 2015, Ukraine witnessed a cyber-attack that resulted in loss of power to over 225,000 of its citizens. Businesses that rely on electrical power, such as transportation systems and hospitals, are the crux of concern of the kinetic effects of a cyber-attack. Cyber security is a growing area of concern due to its economic, social, and environmental impact.

- **The need for diversity in cybersecurity**

There is currently a global surplus of over two million cyber security roles. This global need can be attributed to the shortage of women, minorities, and millennials currently working in cyber security roles. Today, women account for less than 11% of the global cyber security workforce. According to Priscilla Moriuchi, Director of Strategic Threat Development at Recorded Future, "The demand for capable, knowledgeable, hard-working security professionals is so high and the threat to innocent people and critical networks so broad that both women and men can have impactful, rewarding careers in this field." Closing the gender gap within the cyber security workforce will increase the defenses of businesses that possess our private information.



CYBER WORKFORCE DIVERSITY

HOW DO WE GET THERE?

INSPIRE
Encourage and develop positive associations with cyber careers choices

EDUCATE
Share information on specific career paths and training opportunities

RECRUIT
Facilitate career entry or career transition to technical and cyber fields

RETAIN
Provide resources, training, flexibility to grow and retain workforce

ADVANCE
Enable the promotion of workforce from entry level to senior positions

INVEST
Give back to the next generation by sharing, inspiring and educating

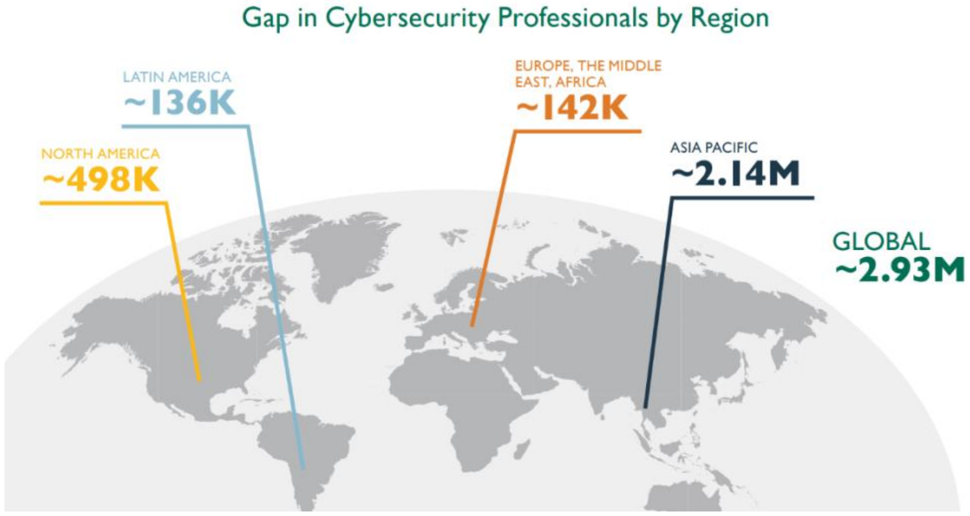
All rights reserved © 2017 Angela Rittenbach, Riverstone Solutions, Inc.

Another underrepresented demographic in the cyber security workforce is African Americans. According to the Bureau of Labor and Statistics, only 3% of information security analyst roles are filled by African Americans. Raising social awareness of the current cybersecurity workforce shortage to minorities will provide career opportunities to millions of African Americans in the future.

Lastly, according to Forbes, only 7% of the cyber security workforce is composed of workers under the age of 29. Wesley Simpson, Chief Operations Officer of (ISC)² states "Over the next 10 years, we will have a large population of cyber professionals starting to retire," Simpson said. "We don't have a good plan to backfill those large number of folks starting to leave the industry." In order to address the growing demand for cyber security professionals, businesses should augment their recruiting efforts to attract millennials.

- **The global need for certified professionals**

Cyber security roles can be both exciting and fulfilling, but as the demand for cyber professionals increases, businesses are unable to find talented individuals to fill these positions. A prime factor to this issue is the lack of cyber security education previously available. Scholastic programs that pertain to cyber security have increased within the United States, with millions of dollars in grants and scholarships also available. The flexibility of online education allows students to continue full-time employment while gaining cyber security proficiency. While these institutions may provide formal education to those with the desire to enter the cyber security workforce, most fail to address a key concern.


Gap in Cybersecurity Professionals by Region
LATIN AMERICA
~136K
EUROPE, THE MIDDLE EAST, AFRICA
~142K
NORTH AMERICA
~498K
ASIA PACIFIC
~2.14M
GLOBAL
~2.93M

Roughly 70% of available cyber security roles require a technical certification. Unlike a diploma, most IT-security certifications require each successful candidate to submit a specified number of continuing education units annually. Given the progressive landscape of modern technology, certifications ensure that cyber security professions are kept abreast on emerging technologies and the threats that each encompass. Certifications also benefit industries that seek competent individuals in a particular subject area. Another key benefit of seeking certified professionals is the adherence to the designating official’s code of professional ethics. An individual’s compliance to ethical standards benefits employers seeking cyber security candidates required for sensitive environments. To promote ethical hires, we must demand certified professionals and provide effective cyber security training to the public.

Key Partnerships

(ISC)^2

The International Information System Security Certification Consortium, or (ISC)^2, is a non-profit organization which specializes in training and certifications for cybersecurity professionals. It has been described as the "world's largest IT security organization". The most widely known certification offered by (ISC)^2 is the Certified Information Systems Security Professional (CISSP) certification.

CompTIA

The Computing Technology Industry Association (CompTIA) is a non-profit trade association, issuing professional certifications for the information technology industry. It is considered one of the IT industry's top trade associations. CompTIA issues vendor-neutral professional certifications in over 120 countries.

EC-Council

The International Council of Electronic Commerce Consultants (EC-Council) is a professional organization that certifies individuals in various e-business and information security skills. EC-Council is best known for its professional certifications for the IT security field. It's certifications CEH, CHFI, CCISO, CND are ANSI accredited.

Navy SEAL Foundation

Since the attacks of Sept. 11, 2001, there has been an unprecedented demand for our Special Operations Forces. Never before has so much been asked of so few, from so many, for so long. The Navy SEAL Foundation provides a comprehensive set of programs specifically designed to improve health and welfare, build and enhance resiliency, empower and educate families and provide critical support during times of illness, injury, loss and transition.

Winvale

Founded in 2003, Winvale is strategically headquartered in the Washington, D.C. area. Supporting more than 3,000 commercial and government organizations. Winvale is recognized as the leading provider of Government Contract Consulting to government contractors across all industries and disciplines. Winvale serves executives and managers by providing expert guidance and support as they enter and compete within government markets.

Customer Service

Cyber Brain Academy provides you with a customer engagement specialist throughout the duration of your training experience, at no additional cost. Cyber Brain Academy is dedicated to your satisfaction. After you complete your five days of instructor-led training, our engagement specialist will contact you with an optional survey to help us evaluate both our curriculum and our instructors, to ensure that we maintain the highest standard of quality.