





How to Win the Cybersecurity Talent Race

trilogyed.com/enterprise
646-618-8898
enterprise@trilogyed.com

Table of Contents

▷ Introduction	1
▷ Cybersecurity Penalties Rise Under Mounting Privacy Regulations	4
▷ The Cybersecurity Career Pathway	13
▷ Cybersecurity Training and Development for the Modern IT Practitioner	16
▷ About Trilogy Education	22



A stylized eye icon in shades of blue and grey, positioned on the left side of the slide, partially overlapping the 'M' in 'MEMBER'.

MEMBER

SECURITY

Introduction

By Kevin W. Yoegel

Data production, collection, usage, and storage are part of daily life for consumers and organizations engaged in the modern digital environment.

All stakeholders involved in this cycle share a similar goal: keep data, and particularly personal data, private and secure. “Data privacy” is not only a meritorious goal but also a legal requirement as many countries and states enact data protection laws. As federal, state, and international government promulgates sweeping privacy legislation, security teams must coordinate the technical deployment of internal policies and procedures to protect data. Failing to protect data can result in incredible remediation costs, loss of customer goodwill, regulatory scrutiny and fines, and, in some cases, even put an organization’s viability in jeopardy.

The impact of data breaches is further evolving as new legislation allows for additional remedies, such as the private cause of action for affected consumers. Most organizations realize the importance of data privacy. The challenges, however, come when developing answers to the question, “How do we get there?”

A robust cybersecurity program is a critical part of this solution. Indeed, many countries, states, and industries have specific information security program requirements, and failure to comply can result in

an assortment of fines and penalties. However, an organization’s cybersecurity program is only as strong as the individuals who implement, deploy, monitor, and enforce it. The demand for cybersecurity professionals in the workforce cannot be understated.

Businesses, consulting firms, and government agencies alike are engaged in constant competition to recruit and retain cybersecurity talent. As threats grow and become more persistent and complex, prospective employees who can become experts in security, threat detection, and incident response will remain in high demand.



Top Five Emerging Organizational Risks

1. **Accelerating privacy regulation**
2. **Pace of change**
3. **Talent shortage**
4. **Lagging digitization**
5. **Digitization misconceptions**

Source: Gartner (April 2019)

Accordingly, to keep their data safe and secure and remain fully compliant with applicable legal frameworks, organizations are actively developing proactive and reactive strategies for security. Proactive strategies include security engineering, secure network architecture design, auditing and penetration testing, compliance, threat hunting, and employee training. Reactive solutions include digital forensics, incident response and management, and business continuity implementation.

An ideal approach blends these aspects of security. With so many specific roles in the field, job candidates have the opportunity to find what best suits their skill sets and interests. The ultimate job responsibility remains the same: protecting the confidentiality, integrity, and availability of protected data within the organization's digital environment. As chief security officers, chief information security officers, and chief information officers are constantly looking for innovative ways to build their teams, the demand for trained information systems security and cybersecurity professionals to fill those roles continues to increase.

A creative way in which organizations are filling this void is by capitalizing on opportunities to retrain and retool. A career in cybersecurity is a perfect pivot for information technologists who want to leverage their prior experience. However, a background in information

technology is not a prerequisite to launch a career in security. A genuine interest and curiosity about computers, networks, and cyberspace, combined with a desire to study and learn, can jump-start a career in the field.

Careers in information systems security and cybersecurity are both stimulating and challenging. Security professionals are in the trenches, constantly striving to keep their organizations safe and operational. The field is cutting edge and rapidly developing with all signs pointing toward continued growth.

As you read this ebook, do not underestimate the value of enhancing your organizational security posture and reducing information system vulnerabilities. Risks and liabilities can be substantially mitigated with due diligence and the proper personnel in place. Take action now by evaluating your teams. Consider career pathways for your incumbent workforce to be reskilled and win the cybersecurity talent race.

Kevin W. Yoegel, CIPT, is a Data Privacy and Cybersecurity Attorney at Lewis Brisbois Bisgaard & Smith LLP, where he advises clients on proactive data privacy and security as well as incident response management and remediation.

"A creative way in which organizations are filling this void is by capitalizing on opportunities to retrain and retool. A career in cybersecurity is a perfect pivot for information technologists who want to leverage their prior experience. "

1 | Cybersecurity Penalties Rise Under Mounting Privacy Regulations

READ THE PRIVACY POLICY

The security of your data is extremely important to us. Thank you for your trust in Paragon.

Kind regards,

Paragon

Senior-level executives remain on edge as new federal, state, and international privacy regulations intensify the consequences of a cybersecurity breach. According to IBM Security, the average cost of a cyber attack in 2018 was about \$3.9 million. Even then, many organizations never fully recovered. Today, the stakes are even higher.

International laws, such as Europe's General Data Protection Regulation (GDPR), can now impose penalties as high as four percent of a company's total annual revenue. State regulations, such as The California Consumer Privacy Act (CCPA), can fine a company as much as \$7,500 per violation. Even specific industries are susceptible to targeted penalties, like Alabama's Insurance Information Security Program Requirement, which aims to improve cybersecurity and data privacy standards in the state's insurance sector.

The mounting risks of a data breach are compounded by our growing cyber-attack surface and the cybersecurity talent shortage. According to ISC2, there is a gap of almost 3 million unfilled cybersecurity positions globally, the likes of which contribute to a lack of security depth in many organizations, which slows implementation and response times. To illustrate the gravity of this situation, let's examine four of the most consequential cybersecurity breaches in recent history. In every case, stronger internal cybersecurity practices could have prevented devastating financial losses.





Marriott

Marriott International runs about 6,000 hotels in 127 countries. In 2016, it purchased Starwood Hotel & Resorts Worldwide in an attempt to become the largest hotel company in the world. Unfortunately, Marriott also bought a massive security issue. At the start of 2018, Marriott's net worth was over \$51 billion. After announcing to the public that their reservation systems had been hacked, exposing hundreds of millions of guest records, the company's net worth plummeted to less than \$38 billion.¹ Not surprisingly, shares also took a 5.6% dive.²

The Cause

A Remote Access Trojan (RAT) went undetected by the hotel's cybersecurity controls, allowing hackers to covertly access, surveil, and siphon information from their reservation database for over four years.

The Fallout³

- 383 million exposed guest records
- 25.55 million stolen passport numbers
- 8.6 million jeopardized credit/debit cards

¹macrotrends (<https://www.macrotrends.net/stocks/charts/MAR/marriott/net-worth>)

²Market Watch (<https://www.marketwatch.com/story/marriotts-stock-sinks-after-disclosing-data-breach-affecting-up-to-500-million-guests-2018-11-30>)

³Cybersecurity Insiders (<https://www.cybersecurity-insiders.com/marriott-hotel-discloses-official-cyber-attack-figures/>)

The Consequences^{4,5,6,7}

- Up to \$915 million in penalties imposed by GDPR
- Up to \$2.8 billion in federal fines to replace stolen passport numbers
- Proposed jail time for senior executives
- Legal fees associated with 100 class action lawsuits

Cybersecurity insurance only covered \$25 million of the multi-billion dollar incident.⁸

⁴Forbes (<https://www.forbes.com/sites/yiannismouratidis/2019/01/09/gdpr-may-add-up-to-8-8b-marriotts-data-breach-expenses/#50c5c40462e1>)

⁵CSO (<https://www.csoonline.com/article/3324255/us-senator-proposes-jailing-execs-fining-companies-for-data-breaches.html>)

⁶Market Watch (<https://www.marketwatch.com/story/after-massive-hack-marriott-pledges-to-pay-for-new-passports-if-fraud-has-taken-place-2018-12-03>)

⁷Marriott 2018 Annual Report (<https://marriott.gcs-web.com/static-files/8799734e-b9e0-4e53-b194-7bd24a381118>)

⁸Security Week (<https://www.securityweek.com/data-breach-cost-marriott-28-million-so-far>)



Under Armour

In 2015, Under Armour reached an all-time high net worth of \$22.5 billion. In just two years, it plunged to a net worth around \$5.5 billion. The timing couldn't have been worse for the company to discover that its popular fitness tracking app, MyFitnessPal, had been hacked. Almost immediately, shares dropped by 4.6%.

The Cause

Without proper cybersecurity protocols in place, MyFitnessPal only encrypted some user passwords with a strong security method called "bcrypt." The rest were encrypted with a weaker hashing scheme called SHA-1, leaving accounts vulnerable to hackers.

The Fallout

- 150 million compromised user accounts (including email addresses and passwords)
- Stolen user information listed for sale on the Dark Web

The Consequences

Under Armour claimed protection under the app's terms and conditions of use. However, a class-action lawsuit has been filed with the California federal court to hold the company accountable for the theft and resale of private user information on the black market.⁹

Had today's privacy regulations been in place at the time of the incident, Under Armour might have also been on the hook for \$110 million or more under GDPR and \$375 billion, give or take, from CCPA.

⁹ Case Document (<https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/under-armour-breach-complaint.pdf>)



Duke Energy

In 2019, Duke Energy became the recipient of the largest fine ever doled out to an energy company after numerous physical and cyber security violations were disclosed to the North American Electric Reliability Corporation (NERC), a constituent of the Federal Electric Regulatory Commission (FERC). Duke Energy self-reported a majority of the violations, except for 16 infractions uncovered during a Critical Infrastructure Protection audit.

The Cause

- Lack of managerial oversight
- Process deficiencies
- Inadequate training
- Lack of internal controls
- Lack of compliance program

The Fallout¹⁰

- An estimated 127 security violations
- Unsecure critical cyber assets

The Consequences

A \$10 million fine was issued by NERC for cybersecurity failures on the grid. Duke Energy is also responsible for remediation to correct security infringements, which may cost as much as \$137.4 million.¹¹

¹⁰ Utility Dive (<https://www.utilitydive.com/news/duke-fined-10m-for-cybersecurity-lapses-since-2015/547528/>)

¹¹ Charlotte Business Journal (<https://www.bizjournals.com/charlotte/news/2019/04/08/why-duke-energys-proposed-137-4m-cybersecurity.html>)

Uber

Uber Technologies

Uber fell on tough times in 2016 after sexual abuse allegations and negative press resulted in a \$2.8 billion loss for the year.¹² The company put a positive spin on the nose-dive, touting exceptional growth rates. However, the company's annual financial report for 2017 revealed a staggering 61% increase in losses, totaling \$4.5 billion for the year.¹³

In Q4 of 2017, the company also announced a large-scale cybersecurity breach that took place in 2016 and compromised the personal information of tens of millions of Uber riders and drivers. Instead of disclosing the breach to authorities and the public, the company chose to pay hackers \$100,000 to destroy the records and keep quiet.

The Cause

Uber developers "cleverly" stashed their login credentials for the company's data stores within their coding on GitHub, a platform used for code management and collaboration. A Florida man successfully obtained the login credentials, hacked the systems, and demanded a ransom.

The Consequences¹⁴

- \$148 million settlement
- \$491,000 fine issued by the UK
- \$678,780 fine issued by the Dutch Data Protection Authority (DPA)
- Uber's CSO was fired

- Uber's CEO resigned
- Social media started a #DeleteUber viral boycott
- Lawsuits filed by Attorneys General from all 50 states
- Private party lawsuits in at least 19 cities

The Fallout¹⁵

- 50 million exposed rider accounts
- 7 million exposed driver accounts
- 600,000 stolen driver's license numbers
- Failure to report the incident within 72 hours

¹² Bloomberg (<https://www.bloomberg.com/news/articles/2017-04-14/embattled-uber-reports-strong-sales-growth-as-losses-continue>)

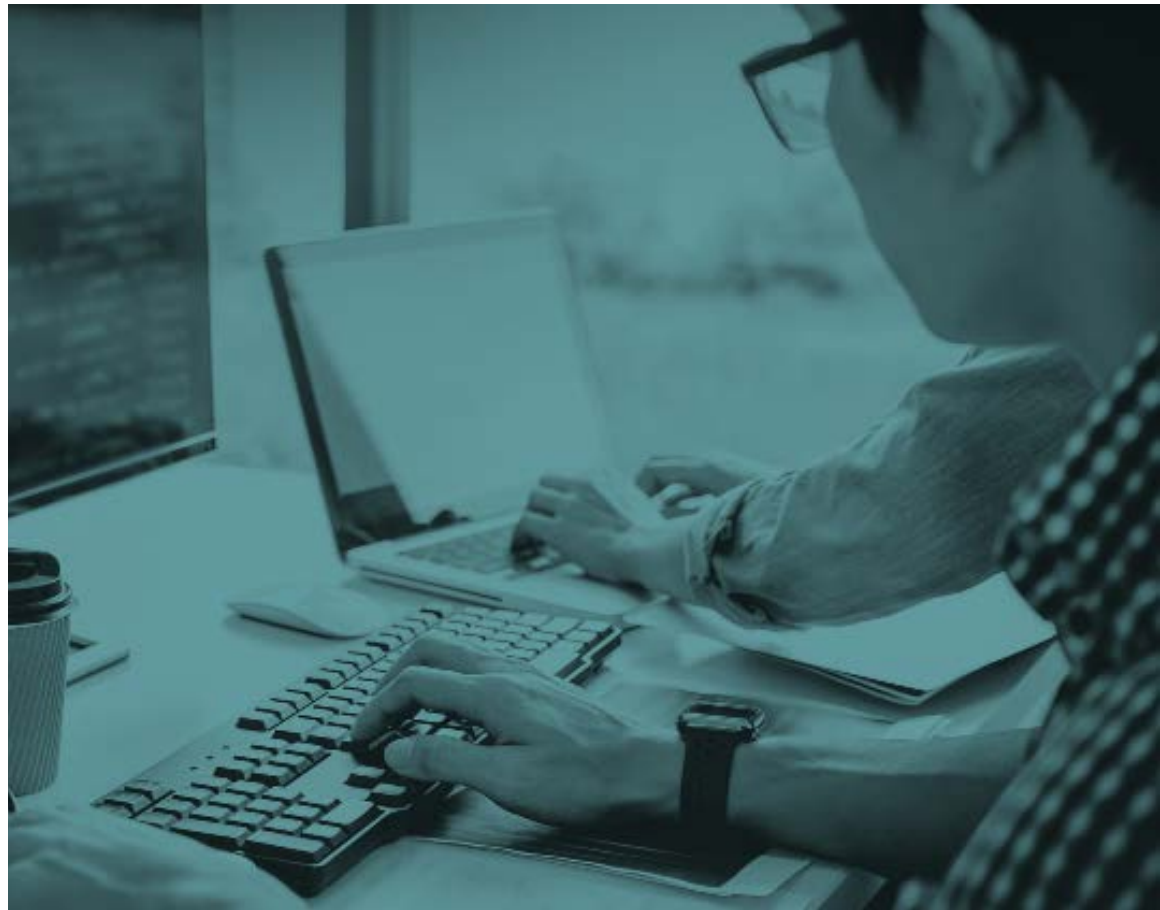
¹³ PYMNTS (<https://www.pymnts.com/earnings/2018/uber-q4-earnings-losses/>)

¹⁴ Reuters (<https://www.reuters.com/article/us-uber-fine/british-dutch-regulators-fine-uber-for-2016-data-hack-idUSKCN1NW0VR>)

¹⁵ npr (<https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach>)

In each of these cases, a lack of internal cybersecurity controls, protocols, and compliance initiatives directly resulted in vulnerabilities that were highly-preventable. These were not sophisticated attacks; they were opportunistic, which places a greater share of the cost on the offending company rather than a cybersecurity insurance policy provider.

As regulators continue to develop new cybersecurity and data privacy laws to protect consumer data, organizations that cannot keep pace will get caught in the crossfire. You cannot depend on just new talent to drive organizational change nor bank on cybersecurity insurance to offset costs. An effective way to protect your digital borders is to implement an education program for technical and non-technical employees, and reskill novice or experienced practitioners to improve your company's cybersecurity agility and adaptability.



2 | The Cybersecurity Career Pathway



The world is becoming more digitally connected. In the past decade, we have seen the rise of affordable and available cloud computing as well as smart devices interconnecting our work and home resulting in massive amounts of data being transmitted and collected. Modern businesses depend on their technology infrastructure to operate. Any disruption to a company's tech systems carries substantial legal and financial risks.

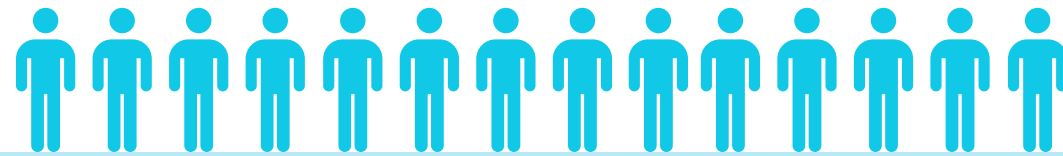
Cybercriminal activity is the fastest growing crime globally. Advances in technology are allowing businesses to behave in sophisticated, automated ways while these same technologies are empowering cybercriminals to increase in size and sophistication at lower costs. Some estimates predict that by 2021 cybercrime damages will exceed the global trade of all illegal drugs.

A major contributing factor to the rise in cybercrime is not only the need to cost-effectively leverage technology at scale but also the ability for the perpetrators to go unnoticed. The rise of cryptocurrency has allowed cybercriminals to get paid anonymously, substantially reducing the risk of being caught. Hacking tools and kits that enable digital crimes such as malware, ransomware, and identity theft can be purchased online at price points less than a fast food value meal. The cost of entry into cybercrime is essentially cheaper than a burger, fries, and a soda.

496,000

US cybersecurity job postings in 2018.

Source: Burning Glass Technologies



of cybersecurity professionals believe that no more than half of applicants for cybersecurity positions are qualified.

Source: ISACA

Ransomware, in particular, has become the fastest growing type of cybercrime, prompting the US Department of Justice to describe it as “[a new business model for cybercrime](#).” The FBI estimates that 100,000 computers a day around the world are infected by ransomware, which could account for \$11.5B in losses in 2019 and is predicted to double by 2021.

The rapid rise in global cybercrime has exacerbated the current shortage of cybersecurity talent. According to the Information Systems Audit and Control Association (ISACA), 69% of cybersecurity professionals believe their teams are understaffed, while 32% of organizations aren’t able to fill open positions for at least six months.

Data from [Burning Glass Technologies](#), an analytics software company that provides real-time information on job growth and labor market trends, reveals that there were more than 496,000 cybersecurity job postings in 2018, up 33% from the prior year. In addition, according to ISACA, 60% of cybersecurity professionals believe that only 50% or less of the applicants applying to open cybersecurity positions are qualified.



Two contributing factors to this dilemma are:

- 1. skills are getting out of date faster**
- 2. traditional education programs struggle to keep up with developments in the industry.**

The ongoing high demand for information and network security skills means that companies need to start looking for new ways to attract cybersecurity talent. According to Burning Glass, companies require specialized skills such as Python, Linux, and Java for both cybersecurity jobs and software development roles. While consumer boot camps have the potential to be one source of junior cybersecurity talent, you need to start developing a cybersecurity career pathway for existing employees.

3

Cybersecurity Training and Development for the Modern IT Practitioner



By Chuck Mackey

Today's uber-crisis world demands a better way to ensure offensive and defensive cybersecurity success. All organizations need to be adaptive in this highly volatile environment. They must sense and rapidly respond to critical incidents, threats, vulnerabilities, and opportunities well before they happen.

Additionally, business success comes from an enterprise's ability to codify, transform, protect, and successfully apply data for economic, social, and communal gain at an always-increasing pace. Protecting an organization's data assets takes more than merely deploying a mass collection of point-specific technology solutions; it requires a top-down strategic and tactically-administered approach that involves targeted skills. It starts and ends with the person who chooses, deploys, uses, and manages modern security tools and technologies: the engaged cybersecurity practitioner.

Both the organization and the contributing practitioner need a comprehensive pathway that enables technical and non-technical education and training—as well as proven leadership and team-building—to obtain the necessary skills for the organization to be resilient in the face of cybersecurity threats. A flexible program allows each practitioner to jump into the pathway regardless of their current skill set or experience level.

Reskilling a novice or experienced practitioner can be done through a four-stage process that I developed when implementing large-scale enterprise applications

during the late 1990s and early 2000s. It remains a high-value model for cybersecurity education, training, and technology implementation today.

The process is called FIRM: Foundation, Immersion, Reinforcement, and Mastery. Each stage increases in both breadth and depth and allows participants to enter at any point on the path, depending on their own experience and the organization's requirements.

Regardless of the current state of cybersecurity, for someone just entering the profession or with limited security skills, there are basic, foundation-based skills necessary to learn and command for progression through the FIRM model. Here are some examples of a likely cybersecurity practitioner skill-building roadmap.

Top Cybersecurity or Related Skills

1. Network Security
2. Network Fundamentals
3. Incident Response
4. OS Vulnerabilities and Hardening
5. Security Fundamentals

Source: Trilogy Education Services Industry Insights (May 2019)

Foundation

Foundation Level programs are optimum for someone with demonstrated technical talent but without formal security education and practical experience. Knowing how on-premise data centers, network environments, and endpoint devices such as laptops, desktops, and mobile devices work together is a prerequisite for a career in cybersecurity.

How an organization configures these systems, what tools they use—such as Endpoint Detection and Response (EDR) and Data Loss Prevention—and how they operate and interact are critical components of a foundation-level skill set necessary for the emerging cybersecurity engineer. And while the objective is to thwart intrusions and other bad-actor activity, incidents will happen. Knowing how to respond, collect evidence, and report findings are all mandatory skills for even the junior engineer.

Foundation Level Programs

- Infrastructure and Network Security
- Prevention: System Configuration
- Detection: Breach Identification and Notification
- Response: Incident Response, Evidence, and Forensic Data Collection
- Security Management: Underlying Technologies, Frameworks, Policies/Procedures, and Measurement

Immersion

Many current security practitioners come to the program with years of experience and perhaps one or more certifications. Often, they are looking to specialize in an area of cybersecurity—e.g., penetration testing/vulnerability scanning, deep forensics, and threat hunting—or within particular operating systems and hardware platforms. These individuals should receive highly-specialized, hands-on training.

For instance, someone interested in threat hunting, which is an offensive cybersecurity pathway, will want and need exposure to significant incident use-cases, tools, techniques, technologies, and processes. The example programs below present a likely way for a relatively seasoned practitioner to gain the necessary skill and ability to specialize in one or more cybersecurity domains.

Immersion Level Programs

- Windows Security
- Mac OS Security
- Linux Security
- Intrusion Detection
- Penetration Testing (Ethical Hacking): Networks and Applications
- Incident Response and Threat Hunting

- Endpoint Detection/Response and Forensics
- Advanced Cyber Security Practitioner
- Cloud Security

Reinforcement

As the individual's skill set grows and his/her experience levels mature, the practitioner will want to handle more challenging activities. The Reinforcement roadmap provides just that. More and more organizations are moving to the cloud, infrastructure-as-a-service, platform-as-a-service, and software-as-a-service. Consequently, new issues arise, and the complexity of both technology and regulatory compliance demand that the cybersecurity engineer reach new heights not just in technical know-how but also in governance, risk, and compliance.

Knowing what to look for, how to integrate disparate security tools, and how to stand up to scrutiny from regulators are skills in high demand today. Working directly with software developers on secure coding practices, especially as web-based applications and application program interfaces (API) become more and more prevalent, is critical for the experienced practitioner.



Most In-Demand Cybersecurity Certifications

- **CompTIA Security+**
- **Certified Information Systems Security Professional (CISSP)**
- **CompTIA Network+**
- **SANS GIAC Certifications**

Source: Trilogy Education Services Industry Insights
(May 2019)

Reinforcement Level Programs

- Advanced Cyber Security Practitioner (Certified Enterprise Resiliency Practitioner, CERP)
- Cloud Security
- Security in Virtualized Environments
- Security Information and Event Management (SIEM)
- Critical Security Controls
- Advanced Penetration Testing: Networks
- Advanced Penetration Testing: Web Applications
- Advanced Penetration Testing: Wireless
- Advanced Penetration Testing: Mobile
- Intro to Specialized Languages (Python, Rails, etc.)
- Digital Forensics
- Malware Analysis
- Threat Intelligence
- Secure Web Applications
- Secure DevOps

Mastery

Terms such as “security ninja” and “guru” are bandied about quite frequently these days. While there are certainly practitioners who live up to the billing, a critically deep understanding of technology and business acumen are required to be considered a master in the field of cybersecurity.

Business leaders, executive management, and even boards of directors are strikingly aware of the significant challenges being placed on their organizations, whether from threat vectors, auditors, or regulators. Due to this general awareness, the cybersecurity master must have full command of the technology, understand how cybersecurity technology differs from other technologies within the organization, and comprehend how cybersecurity prioritization is a force multiplier in protection and regulatory adherence.

Whether a senior-level cybersecurity engineer, chief information security officer (CISO), or cybersecurity team leader, today’s practitioner must be nimble, forthright, and confident that the recommendations and decisions s/he makes can stand up to economic challenges and resource constraints.

The Master Level program expressly prepares the seasoned cybersecurity practitioner for more and more responsibility and the commensurate authority to take on the ever-increasing complexities of cybersecurity.

Master Level Programs

- Secure Coding: Language Specific Workouts
- Physical Security
- Planning, Policy, and Governance
- Role of Board of Directors
- Red Team / Blue Team Operations
- Securing Data
- Breach/Incident Investigation

The FIRM model is not an end-all-be-all. It is, however, a robust and practical approach to improving the secure position and posture of an organization through an education and training program proven to be effective in the field and the classroom.

Chuck Mackey manages the Data Protection Office for AmTrust Financial Services, Inc. He has consulted regularly on IT security matters for Big Four consulting firms, higher education institutions, government agencies, and the private sector.





About Trilogy Education

About Trilogy Education

Trilogy Education is a workforce accelerator that provides skills-based training programs to bridge regional hiring gaps in software and web development, data analytics, UX/UI, cybersecurity, and other high-demand technical skills in more than 40 markets around the globe.

Trilogy has helped more than 2,500 companies fill their employment gaps. As companies continue to hire multiple Trilogy university-powered boot camp graduates, more of them request corporate training programs that help ACQUIRE a diverse pipeline of technical talent or RESKILL or UPSKILL technical or non-technical teams to meet current and future business needs.

Measurable program outcomes include:

- Reduce the time and expense to acquire new employees
- Improve workforce engagement
- Provide career advancement opportunities
- Boost employee retention

Trilogy has earned the support from the world's leading universities that lend their expertise and oversight to the delivery of every program. As a measure of the quality and rigor, participants receive a university certificate upon successful program completion.





TRILOGY
EDUCATION SERVICES

trilogyed.com/enterprise
646-618-8898
enterprise@trilogyed.com

All statements in this ebook attributable to Gartner represent Trilogy Education Services' interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this ebook). The opinions expressed in Gartner publications are not representations of fact and are subject to change without notice.

Confidential & Proprietary Information of Trilogy Education Services © Trilogy Education Services, a 2U, Inc. brand.