A guide for New Cybersecurity Enthusiasts.

By Jeaniffer

Table of Contents

About the Creator of This Guide

Jeaniffer, a cybersecurity professional, embarked on this dynamic journey in 2019. Her academic foundation in Political Science from Texas A&M University set the stage for a different trajectory. Initially aimed at pursuing Law School post her Bachelor's degree in 2017, her aspirations took a transformative turn when she discovered her passion for cybersecurity through her husband.

Driven by an insatiable curiosity and dedication, Jeaniffer graduated summa cum laude from the University of Dallas with a Master's degree in Cybersecurity in 2022. Her commitment to excellence led her to achieve industry certifications including CompTIA Security+, AWS Cloud Practitioner, and (ISC)² CC, solidifying her expertise.

Currently serving as an Information Security Engineer at a Fortune 500 company, Jeaniffer embodies a fervent dedication to fortifying digital landscapes and safeguarding against evolving threats.

This guide is a comprehensive resource of all the research she has done over the years. It answers where someone should begin when diving into this field and beyond.
This guide aims to provide insightful answers to the very questions many individuals like herself once had while navigating a transition into cybersecurity. It's a roadmap that not only illuminates the initial steps but also offers guidance on the multifaceted aspects of this field, catering to those contemplating or embarking on a career path.

Did you know this guide is interactive? Links are annotated with underlines and will lead to websites.

Follow Jeaniffer on social media
Instagram
Donate to the Jeaniffer Foundation

Understanding Cybersecurity

What is Cybersecurity?

Cybersecurity is the practice of protecting computer systems, networks, devices, and data from unauthorized access, cyberattacks, damage, or theft. It involves a range of technologies, processes, and practices designed to safeguard information and prevent disruption to digital services.

Significance of Cybersecurity

Understanding the significance of Cybersecurity and its various aspects is crucial for anyone looking to enter this field.

In today's interconnected world, nearly every aspect of our lives relies on digital technology. From personal communication to critical infrastructure, businesses, and governments, our dependence on digital systems is pervasive.

Cybersecurity ensures the protection and proper functioning of these systems, and guarding against potential threats that could disrupt daily operations or compromise sensitive information.

Aspects of Cybersecurity

Cyber threats are continually evolving. They encompass a wide array of methods, including ransomware, phishing, social engineering, and more. Hackers constantly develop new techniques to exploit vulnerabilities, making cybersecurity a continuous challenge that requires proactive measures to detect, prevent, and respond to these threats effectively.

Importance of Protecting Data and Systems

Successful cyber attack can lead to financial losses, reputational damage, and compromise personal or organizational data. For businesses, a successful cyber attack can disrupt operations, halt services, and erode customer trust. For individuals, it can result in identity theft, financial fraud, or exposure of sensitive personal information, causing significant distress and potential long-term repercussions.

Education and Learning Paths

The famous Degree v. Bootcamp v. Self-learning debate

If you are active on X (formerly Twitter), the debate of whether to pivot into Cybersecurity through a degree, boot camp, or self-learning resources like Udemy is intense. Now, I am not here to add to that argument or state which is better because I did all three.
In this section, we are going to dive deeper into different educational paths and learning options in cybersecurity, and then you can choose which option works best for you. In my honest opinion, no option is better than the other, but I do prefer Udemy as it is cheaper.

Additionally, the option you choose depends on your career goals. If you are seeking managerial or leadership roles, a formal degree might be your best option. Those seeking an entry-level position, or want to focus on quickly and cost-effectively gaining practical skills might go for a boot camp. Finally, for professionals seeking to enhance a specific skill or go after a certification, self-learning is best. I always prefer Jason Dion's course in Udemy as he not only talks about the certification objectives but provides real-world applications.

In all, each educational path has its strengths and weaknesses, and the choice should align with your career goals, time availability, financial considerations, and preferred learning style. Combining multiple learning paths or supplementing formal education with online courses and self-learning can create a well-rounded cybersecurity education.
Below, I have listed the pros and cons of each learning path to assist you in your decision-making.

Formal Degrees (Computer Science/Cybersecurity)

Pros:

- Formal degrees offer comprehensive education covering various aspects of cybersecurity, including theory, practical applications, and hands-on experience.
- Universities provide opportunities to network with peers, professors, and industry professionals, creating valuable connections.
- Degrees from accredited institutions often carry weight in the job market, enhancing credibility.

Cons:

- Pursuing a degree can take several years and involve significant costs, including tuition fees and expenses for books, materials, and living arrangements.
- Some degree programs might have a fixed curriculum, limiting flexibility in exploring specific areas of interest within cybersecurity.

Online Courses and Bootcamps

Pros:

- Online courses and bootcamps offer flexibility in terms of scheduling, allowing you to study at your own pace and alongside other commitments.
- Many online platforms offer specialized courses focusing on specific areas within cybersecurity, allowing you to tailor your education.
- Compared to formal degrees, online courses and bootcamps are often more cost-effective.

Cons:

- While some courses can be comprehensive, others might lack depth or practical experience compared to formal degrees.
- Not all online courses or bootcamps carry the same recognition as degrees from accredited institutions, potentially affecting job prospects.

Self-Learning Resources (Cybrary, Coursera, Udemy, etc.)

Pros:

- Self-learning platforms offer a wide array of resources accessible globally, providing a vast pool of knowledge.
- Many self-learning resources are affordable or even free.
- Learners can target specific skills or areas of interest within cybersecurity.

Cons:

- Self-learning requires discipline and self-motivation, lacking the structured learning environment of formal education.
- While some platforms offer certifications, the recognition of these credentials may vary in the job market.

SELF ASSESSMENT

Don't know if you want to explore a technical or non-technical role in cyber? Here's a quick quiz to assess your strenghts.

Cybersecurity Role Inclination Quiz

1= STRONGLY DISAGREE

3= NEUTRAL

5= STRONGLY AGREE

Rate each statement from 1-5 based on how much you agree.

Tally up your scores for each section:

25-30: Strong inclination towards technical roles in cybersecurity

20-24: Balanced interest; explore both technical and non-technical roles further.

15-19: Leaning towards non-technical roles within cybersecurity.

Below 15: Your strengths might align more with non-technical roles in cybersecurity.

Technical Role:

1. I enjoy exploring the technical aspects of computers, networks, and software.
2. Learning programming languages interest me.
3. Troubleshooting technical issues excites me.

Problem-Solving and Analytical Thinking:

4. I'm skilled at dissecting complex problems and finding innovative solutions.
5. Analyzing patterns and data comes naturally to me.
6. I enjoy tackling challenging puzzles or problems.

Policy and Compliance Interest:

7. Understanding legal aspects or compliance requirements intrigues me.
8. I see value in creating security policies or procedures.
9. I'm interested in ensuring organizations adhere to cybersecurity regulations.

Technical Paths

Upon completing your self-assessment on page 6, if your interests and score align with the technical side of cyber, please explore these roles. By all means, this is not an exhaustive list of all technical roles in cybersecurity. I have only listed a few along with relevant certifications to get your foot in the door.

Penetration Tester

Role: Penetration Testers, often referred to as ethical hackers, evaluate systems, networks, and applications for vulnerabilities and weaknesses.

Technical Skills:

- Proficiency in conducting penetration tests, exploiting vulnerabilities, and performing ethical hacking methodologies.
- Understanding of network protocols, configurations, and security measures to assess and exploit weaknesses.
- Proficiency in scripting languages (Python, Bash, PowerShell, etc.) to automate tasks and develop custom tools.
- Knowledge of web vulnerabilities (SQL injection, XSS) and how to assess and secure web applications.

Relevant Certifications:

- CompTIA Security+: Provides foundational knowledge in security concepts, including network security.
- eLearnSecurity Junior Penetration Tester (eLearnSecurity eJPT): Entry-level certification focusing on penetration testing skills for beginners.
- Certified Ethical Hacker (CEH): Covers ethical hacking techniques, tools, and methodologies.
- Offensive Security Certified Professional (OSCP): Requires practical hands-on examination, validating skills in penetration testing and exploitation.

Incident Responder

Role: Incident Responders detect, analyze, and respond to cybersecurity incidents within an organization, aiming to minimize the impact of security breaches.

Technical Skills:

- Ability to collect, analyze, and interpret forensic evidence following security incidents.
- Knowledge of incident response frameworks (e.g., NIST) and procedures for managing security incidents.
- Understanding malware behavior, analyzing code, and creating countermeasures.
- Effective communication during incident response, collaborating with teams, and reporting findings.

Relevant Certifications:

- GIAC Certified Incident Handler (GCIH): Covers incident handling and response skills.
- GIAC Security Essentials (GSEC): Covers a broad range of information security topics, including incident response.
- Certified Incident Handler (GCIH): Covers incident handling and response skills.
- CompTIA Cybersecurity Analyst+ (CySA+): Covers behavioral analytics, threat intelligence, and incident response.
- EnCase Certified Examiner (EnCE : Specialized in digital forensic analysis and evidence collection using EnCase software.

Network Security Engineer

Role: Network Security Engineers design, implement, and maintain secure networks, ensuring the protection of organizational assets.

Technical Skills:

- Understanding of firewalls, IDS/IPS, VPNs, and secure network architecture design.
- Knowledge of secure software development and common vulnerabilities (OWASP Top 10).
- Ability to configure and secure operating systems, patch management, and access control.
- Skills in analyzing security incidents, conducting forensics, and mitigating security breaches.

Relevant Certifications:

- CompTIA Network+: Covers fundamental networking concepts, addressing, and troubleshooting.
- Cisco Certified Network Associate - Security (CCNA Security): Covers foundational knowledge in securing Cisco networks.
- Certified Network Security Professional (CNSP): Covers network security principles, architecture, and solutions.
- Certified Information Systems Security Professional (CISSP) Associate: While CISSP is advanced, earning an associate status can indicate readiness for the full certification.

Technical Paths

Cryptographer

Role: Cryptographers focus on designing and analyzing cryptographic systems to secure data and communications.

T**echnical Skills:**

- Understand number theory, algebra, and probability theory.
- Knowledge of encryption algorithms (AES, RSA), hash functions, and cryptographic protocols (SSL/TLS).
- Ability to implement cryptographic algorithms and protocols in software and hardware.

Relevant Certifications:

- Certified Cryptography Professional (CCP): Covers cryptographic principles, algorithms, and their applications.
- Certified Encryption Specialist (CES): Emphasizes encryption techniques and their practical implementation.

Security Architect

Role: Security Architects design and build secure systems, networks, and applications, ensuring they meet security requirements and standards.

Technical Skills:

- Identify and mitigate security risks in systems and applications.
- Understand system design, network architecture, and security principles.
- Knowledge of security frameworks, compliance, and regulations.

Relevant Certifications:

- Certified Information Systems Security Professional (CISSP): Covers security architecture, risk management, and security engineering.
- Certified Information Security Manager (CISM): Focuses on information risk management and governance.

Malware/Reverse Engineer

Role: Malware Analysts dissect and analyze malicious software, understand its behavior, and develop countermeasures to defend against it.

Technical Skills:

- Proficiency in using tools to analyze malware behavior and understand its code.
- Ability to deconstruct code to identify malware functionalities and vulnerabilities.
- Understand various Operating Systems (OS) internals to analyze malware behavior across platforms.

Relevant Certifications:

- GIAC Reverse Engineering Malware (GREM): Covers reverse engineering skills for analyzing and combating malware.
- Certified Malware Investigator (CMI): Covers techniques for investigating and responding to malware incidents.

Technical Paths

Security Operations Center (SOC) Analyst

Role: SOC Analysts monitor and respond to security incidents, analyze threats, and ensure the security of an organization's systems.

Responsibilities:

- Monitor security alerts and analyze potential threats.
- Investigate and triage security incidents.
- Implement and maintain security tools and technologies.

Technical Skills:

- Proficiency in using Security Information and Event Management (SIEM) tools for log analysis and threat detection.
- Ability to identify and respond to security incidents, following incident response procedures.
- Understand threat landscapes, attack vectors, and emerging threats.

Relevant Certifications:

- CompTIA Security+: Covers basic security concepts and incident response.
- Certified SOC Analyst (CSA): Covers SOC operations, threat hunting, and incident response.
- GIAC Certified Incident Handler (GCIH): Covers incident handling and response skills.

IoT Security Specialist

Role: IoT Security Specialists focus on securing Internet of Things devices and networks, addressing vulnerabilities in connected devices.

Responsibilities:

- Evaluate security posture of IoT devices, sensors, and gateways within an organization's infrastructure.
- Conduct risk assessments and identify security gaps in IoT architectures and communication protocols.
- Develop and implement security measures and protocols tailored to IoT environments.

Technical Skills:

- Understand IoT device architectures, protocols (MQTT, CoAP), and communication standards.
- Ability to identify and address security flaws in IoT devices and networks.
- Implement security controls specific to IoT environments.
- Knowledge of risk assessment methodologies and strategies in IoT deployments.

Relevant Certifications:

- Certified IoT Security Practitioner (CIoTSP): Covers securing IoT environments, risk management, and compliance.
- IoT Security Foundation Certified Practitioner: Covers IoT security principles, design considerations, and best practices.

Cloud Security Engineer

Role: Cloud Security Engineers focus on securing cloud-based infrastructures and services.

Responsibilities:

- Design and implement security measures for cloud environments.
- Ensure compliance with cloud security best practices and standards.
- Monitor and respond to security incidents in the cloud.

Technical Skills:

- Proficiency in securing and configuring cloud platforms (AWS, Azure, GCP).
- Implement secure user access controls and policies.
- Secure data in transit and at rest within cloud environments.

Relevant Certifications:

- Certified Cloud Security Professional (CCSP): Covers cloud security concepts, architecture, and design.
- AWS Certified Security - Specialty: Covers securing AWS environments.

Technical Paths

Application Security Engineer

Role: Application Security Engineers focus on ensuring the security of software applications throughout the development lifecycle.

Responsibilities:

- Develop and implement security automation scripts and workflows.
- Integrate security tools and platforms for automated incident response.
- Monitor and manage security automation processes.

Technical Skills:

- Proficiency in scripting languages (Python, PowerShell) for automating security tasks.
- Knowledge of integrating security tools and platforms using APIs.
- Understanding of DevOps principles and practices for seamless automation.

Relevant Certifications:

- Certified Security Automation Professional (CSAP): Covers security automation strategies and implementation.
- Certified Information Systems Security Automation (CISSA): Covers automation techniques for cybersecurity.

Data Security Analyst

Role: Data Security Analysts focus on safeguarding sensitive data, ensuring its confidentiality, integrity, and availability.

Responsibilities:

- Analyzing and assessing data security risks and vulnerabilities.
- Implementing data encryption and access controls.
- Monitoring data breaches and responding to incidents.

Technical Skills:

- Knowledge of encryption, tokenization, and data masking techniques.
- Understanding of database security best practices and secure data storage.
- Understanding of data privacy regulations (GDPR, HIPAA, etc.).

Relevant Certifications:

- Certified Information Systems Security Professional (CISSP): Covers various security domains, including data security.
- Certified Data Privacy Solutions Engineer (CDPSE): Covers data privacy engineering and compliance.

IAM Specialist

Role: Identity and Access Management (IAM) Specialists manage and control user access to systems and data, ensuring secure and efficient identity management.

Responsibilities:

- Designing and implementing identity management solutions.
- Managing user access, authentication, and authorization.
- Ensuring compliance with access control policies.

Technical Skills:

- Knowledge of IAM tools and technologies for identity provisioning, authentication, and access control.
- Understanding of role-based access control (RBAC) and least privilege principles.
- Implementing single sign-on (SSO) and federated identity solutions.

Relevant Certifications:

- Certified Identity and Access Manager (CIAM): Focuses on IAM strategies, implementation, and governance.
- Certified Authorization Professional (CAP): Covers access control systems and methodologies.

Technical Paths

Security Automation Engineer

Role: Security Automation Engineers focus on automating security processes to enhance efficiency and response capabilities.

Responsibilities:
- Developing and implementing security automation scripts and workflows.
- Integrating security tools and platforms for automated incident response.
- Monitoring and managing security automation processes.

Technical Skills:
- Knowledge of common vulnerabilities and secure coding techniques.
- Proficiency in using tools for static and dynamic application security testing (SAST, DAST).
- Understanding of programming languages and software development frameworks.

Relevant Certifications:
- Certified Application Security Engineer (CASE): Focuses on secure application development practices.
- Certified Secure Software Lifecycle Professional (CSSLP): Covers security best practices throughout the software development lifecycle.

Threat Intelligence Analyst

Role: Threat Intelligence Analysts focus on gathering and analyzing threat data to proactively identify and mitigate potential cyber threats.

Responsibilities:
- Collecting and analyzing threat data from various sources (dark web, threat feeds, etc.).
- Developing threat profiles and assessing potential risks to the organization.
- Providing actionable intelligence to enhance security measures.

Technical Skills:
- Proficiency in analyzing threat data and identifying patterns or trends.
- Knowledge of threat intelligence platforms and tools for data collection and analysis.
- Ability to present complex threat information in a clear and concise manner.

Relevant Certifications:
- Certified Threat Intelligence Analyst (CTIA): Focuses on threat intelligence analysis and threat hunting skills.
- GIAC Cyber Threat Intelligence (GCTI): Validates skills in cyber threat intelligence analysis and response.

Digital Forensics Analyst

Role: Digital Forensics Analysts investigate cyber incidents and cybercrime, collecting and analyzing digital evidence for legal purposes.

Responsibilities:
- Collecting, preserving, and analyzing digital evidence from various sources.
- Conducting forensic examinations on computers, mobile devices, and networks.
- Documenting findings and presenting evidence for legal proceedings.

Technical Skills:
- Proficiency in using forensic tools for data extraction and analysis (e.g., EnCase, FTK).
- Understanding of legal procedures and protocols for evidence collection and handling.
- Ability to recover and reconstruct data from compromised systems.

Relevant Certifications:
- Certified Digital Forensics Examiner (CDFE): Focuses on digital forensics techniques and evidence handling.
- GIAC Certified Forensic Examiner (GCFE): Validates skills in forensic analysis and incident response.

Non-Technical Paths

Upon completing your self-assessment on page 6, if your interests and score align with the non-technical side of cyber, please explore these roles. By all means, this is not an exhaustive list of all non-technical roles in cybersecurity. I have only listed a few along with relevant certifications to get your foot in the door.

Security Analyst

Role: Security Analysts focus on analyzing security threats and vulnerabilities, providing insights to improve an organization's security posture.

Responsibilities:

- Monitoring security alerts and incidents.
- Analyzing security data and trends for potential risks.
- Producing reports and recommendations for security enhancements.

Skills:

- Ability to assess security threats and vulnerabilities.
- Knowledge of risk management methodologies and frameworks.
- Strong communication and documentation skills for presenting findings.

Relevant Certifications:

- CompTIA Security+: Provides foundational knowledge in security concepts and practices.
- ISACA Certified Information Security Manager (CISM): Covers information risk management and governance.

Compliance Officer

Role: Compliance Officers ensure that an organization adheres to relevant laws, regulations, and standards concerning security and privacy.

Responsibilities:

- Ensuring compliance with industry standards and regulations.
- Conducting audits and assessments to validate compliance.
- Developing and implementing compliance policies and procedures.

Skills:

- Understanding of industry-specific regulations (HIPAA, GDPR, etc.).
- Ability to conduct compliance audits and assessments.
- Developing and enforcing compliance policies and procedures.

Relevant Certifications:

- ISACA Certified Information Systems Auditor (CISA): Covers auditing, control, and assurance skills.
- ISACA Certified in Risk and Information Systems Control (CRISC): Cover risk management and compliance.

Policy Developer

Role: Policy Developers create and maintain security policies, procedures, and guidelines to establish and enforce security standards within an organization.

Responsibilities:

- Developing security policies and procedures aligned with industry standards.
- Reviewing and updating existing security policies to reflect changes in threats and regulations.
- Communicating and training employees on security policies and best practices.

Skills:

- Ability to create comprehensive security policies and guidelines.
- Strong communication skills to convey policies and procedures effectively.
- Understanding of risk implications when developing policies.

Relevant Certifications:

- ISACA Certified Information Systems Security Professional (CISSP): Advanced certification covering security policy development and management.
- ISACA Certified Information Security Manager (CISM): Covers information security governance and policy development.

Non-Technical Paths

GRC Analyst

Role: Government Risk, and Compliance (GRC) Analysts ensure that an organization's policies and procedures align with regulatory standards and industry best practices.

Responsibilities:

- Conducting risk assessments and identifying vulnerabilities in the organization's processes and systems.
- Developing and implementing governance frameworks and compliance policies.
- Monitoring and ensuring adherence to security standards and regulations.

Skills:

- Knowledge of risk assessment methodologies and tools.
- Understanding of regulatory requirements and frameworks.
- Ability to create and enforce security policies and procedures.

Relevant Certifications:

- ISACA Certified in Risk and Information Systems Control (CRISC): Focuses on risk management and control monitoring.
- CompTIA Security+: Entry-level certification covering various security domains including risk management and compliance. It also provides foundational knowledge in security concepts, risk identification, and compliance frameworks.
- (ISC)² CGRC: Focuses on risk management, and compliance principles. .

GRC Consultant

Role: GRC Consultants provide advisory services to organizations, assisting in implementing and improving GRC programs.

Responsibilities:

- Advising on GRC strategy and program implementation.
- Conducting GRC assessments and gap analyses.
- Recommending solutions to enhance GRC maturity.

Skills:

- Ability to provide guidance and recommendations.
- Managing GRC implementation projects effectively.
- Communicating complex GRC concepts to stakeholders.

Relevant Certifications:

- Certified Information Systems Security Professional (CISSP): Advanced-level certification focusing on security program development and management.
- ISACA Certified in Risk and Information Systems Control (CRISC): Focuses on risk management and control monitoring.
- ISACA Certified Information Systems Auditor (CISA): Mid-level certification emphasizing auditing, control, and assurance skills.

Cybersecurity Project Manager

Role: Cybersecurity Project Managers oversee security-related projects, ensuring they are delivered on time, within budget, and meet security requirements.

Responsibilities:

- Planning and managing cybersecurity projects and initiatives.
- Coordinating with cross-functional teams for implementation.
- Ensuring compliance with security policies and standards.

Skills:

- Strong skills in project planning, execution, and monitoring.
- Ability to facilitate collaboration among diverse teams.
- Understanding of risk assessment and mitigation strategies.

Relevant Certifications:

- Project Management Professional (PMP): Focuses on project management principles.
- Certified Information Security Manager (CISM): *Optional* CISM includes project management in its domains.

Non-Technical Paths

Data Protection Officer

Role: Privacy Officers or Data Protection Officers (DPOs) ensure an organization's compliance with data protection regulations and manage privacy policies.

Responsibilities:

- Ensuring compliance with data protection laws (GDPR, CCPA, etc.).
- Developing and maintaining data privacy policies and procedures.
- Handling data breach incidents and liaising with regulatory authorities.

Skills:

- Understanding of data protection laws and regulations.
- Ability to develop and implement data privacy strategies and policies.
- Skills in managing and responding to data breach incidents.

Relevant Certifications:

- Certified Information Privacy Professional (CIPP): Focuses on privacy laws, regulations, and compliance.
- Certified Data Privacy Solutions Engineer (CDPSE): Covers data privacy engineering and compliance.

Security Awareness Training Specialist

Role: Security Awareness Training Specialists design and deliver cybersecurity training programs to educate employees on security best practices.

Responsibilities:

- Creating and delivering cybersecurity training materials and workshops.
- Conducting security awareness campaigns and phishing simulations.
- Measuring and evaluating the effectiveness of training programs.

Skills:

- Strong communication and instructional design skills.
- Ability to convey technical concepts in a non-technical manner.
- Assessing the impact and effectiveness of security training.

Relevant Certifications:

- Certified Security Awareness Practitioner (CSAP): Focuses on developing and managing security awareness programs.
- Certified Information Security Manager (CISM): Covers security program development and management.

Vendor Risk Manager

Role: Vendor Risk Managers assess and manage the risks associated with third-party vendors and suppliers.

Responsibilities:

- Evaluating vendor security and assessing potential risks.
- Developing vendor risk management strategies and frameworks.
- Monitoring and ensuring vendor compliance with security standards.

Skills:

- Ability to assess and manage risks associated with third-party vendors.
- Understanding security implications in vendor contracts and agreements.
- Ensuring vendors comply with security and privacy standards.

Relevant Certifications:

- Certified Third Party Risk Professional (CTPRP): Focuses on managing third-party risks and compliance.
- Certified Information Security Manager (CISM): *Optional* CISM includes vendor risk management among its domains.

Non-Technical Paths

Risk Analyst

Role: Risk Analysts identify, assess, and manage cybersecurity risks within an organization.

Responsibilities:
- Conducting risk assessments and analyzing potential threats.
- Developing risk mitigation strategies and recommending controls.
- Collaborating with teams to implement risk management plans.

Skills:
- Ability to evaluate and prioritize security risks.
- Capacity to analyze complex data and trends.
- Strong communication skills to convey risks and mitigation strategies.

Relevant Certifications:
- Certified Information Systems Security Professional (CISSP): Covers risk management among its domains.
- Certified Risk and Information Systems Control (CRISC): Focuses on risk identification and mitigation.

Cybersecurity Auditor

Role: Cybersecurity Auditors evaluate and assess an organization's security controls and policies to ensure compliance and effectiveness.

Responsibilities:
- Conducting security audits and assessments.
- Reviewing security policies and controls for compliance.
- Providing recommendations for improving security posture.

Skills:
- Ability to perform thorough audits and assessments.
- Understanding of security standards and compliance requirements.
- Capability to identify gaps and vulnerabilities in security controls.

Relevant Certifications:
- Certified Information Systems Auditor (CISA): Focuses on auditing, control, and assurance skills.

Cybersecurity Sales Engineer

Role: Cybersecurity Sales Engineers provide technical expertise and support to sales teams, assisting in selling cybersecurity solutions.

Responsibilities:
- Understanding customer requirements and proposing appropriate solutions.
- Providing technical product demonstrations and presentations.
- Assisting in the design and implementation of security solutions.

Skills:
- Understanding of cybersecurity solutions and technologies.
- Ability to articulate technical concepts to non-technical audiences.
- Capability to propose tailored solutions based on client needs.

Relevant Certifications:
- Salesforce Trailhead (Salesforce Certifications): Offers training modules and certifications in sales, customer relationship management, and sales strategies.
- HubSpot Academy Certifications: Provides courses on inbound marketing, sales, and customer service.
- CompTIA Security+: Provides a foundational understanding of cybersecurity concepts.

CHAPTER THREE

Hands on Experience

Internships and Co-Op Programs

Many companies offer internships providing opportunities to work on real projects, and sometimes gain mentorship. My first role in the industry was an internship and fortunately, after the internship was over, I got offered a full-time opportunity afterwards.

Cybersecurity Labs and Simulations

Virtual labs and simulations (e.g., CyberRange Platforms, TryHackMe), simulate real-world scenarios, allowing hands-on practice in a controlled environment.

Capture-the-Flag (CTF) Competitions

CTF events offer challenges simulating security breaches where participants solve puzzles or vulnerabilities to gain points. Temple University's Cybersecurity in Application, Research, & Education (CARE) Lab hosts creative and unique social engineering CTFS. No technical experience is required.

Bug Bounty Programs

Platforms like HackOne or BugCrowd allow individuals to find and report vulnerabilities in applications for rewards, enabling real-world testing. I also want to note that a lot of people in the field gained their experience through bug bounty programs v. getting a traditional FTE role.

Contributing to Open-Source Projects

Engaging in open-source projects enables collaboration, code review, and exposure to real-world security implementations.

Personal Projects and Home Labs

This is an all-time favorite of mine. Creating your own projects or setting up home labs to experiment with various cybersecurity tools and techniques can provide hands-on experience and showcase practical expertise to potential employers.

Continous Learning

Continuous learning is an absolute must if you want to be in Cybersecurity. Threats, vulnerabilities, technologies, and the market evolve and so must you. Below are ongoing learning resources to maintain market relevance. Important tip: **Google is your best friend**. Whatever you do not know, Google is there for you. Be inquisitive and always ask questions.

Blogs and Website

Schneier on Security, Krebs on Security, and The Hacker News offer insights into cybersecurity news, trends, and analysis.

Podcasts and Webinars

- Podcasts like Security Now, Darknet Diaries, and The CyberWire offer discussions on cybersecurity topics, interviews with experts, and real-world incidents.
- Webinars hosted by security organizations and industry leaders provide in-depth insights into emerging threats and technologies.

Industry News Outlets

Reputable news outlets like SecurityWeek, Threatpost, and Infosecurity Magazine provide comprehensive coverage of cybersecurity events, trends, and analysis.

Professional Associations and Certifications

- Engage with industry associations like ISACA, (ISC)², and CompTIA for access to resources, webinars, and industry reports.
- Pursue advanced certifications that require continuous education, ensuring ongoing learning and skill enhancement.

Resources and Tools

Learning Platforms and Websites

Tool Name	Features	Cost
Cybrary	Offers free and paid courses covering a wide range of topics	Free & Paid
Coursera	Provides courses from universities on cybersecurity	Free access to some courses but might require payment for certification.
Udemy	Offers a variety of courses. *Jason Dion is my favorite instructor on this platform.	Free & Paid. *Free courses might have limited content.
edX	Offers cybersecurity courses from renowned universities like Harvard	Free access to some courses but might require payment for certification.
Khan Academy	Provides Introductory cybersecurity courses and resources	Free

Practice Environments and Tools

Tool Name	Features	Cost
Kali Linux	Linux distribution designed for penetration testing and ethical hacking.	Free and open source
Wireshark	Network protocol analyzer for troubleshooting & analysis.	Free and open source
Metasploit	Framework for developing, testing, and executing exploit code.	Free and open-source.
Cobalt Strike	Penetration testing tool used for simulation.	Paid
OWASP WebGoat and Juice Shop	Vulnerable web applications for practicing web security.	Free and open-source.
Cyber Range	Virtual environments for hands-on practice (e.g., RangeForce, Hack The Box)	Free and open-source.

Websites and Communities

Tool Name	Features	Cost
Open Web Application Security Project (OWASP)	Offers tools and documentation on web application security	Free
SANS Institute	Provides trainings and certifications. *Employer's offering SANS training as a benefit? Grab that opportunity with both hands! These courses + certs come with a hefty price tag, but they hold serious weight in the industry*	Paid
Hack Forums	Online community for discussing hacking techniques.	Free
Reddit Communities	Subreddits like r/netsec, r/AskNetsec, and r/cybersecurity provide discussions and Q&A on cybersecurity topics.	Free
Discord Channels	Security-focused servers like Cyber Security Hub, The Many Hats Club, and Red Team Village for discussions and learning.	Free
Books	The Web Application Hacker's Handbook" by D. Stuttard and M. Pinto, Hacking: The Art of Exploitation by Jon Erickson, Practical Malware Analysis by Michael Sikorski and Andrew Honig.	Paid
Podcasts	Darknet Diaries by Jack Rhysider. Defensive Security by Jerry Bell & Andrew Kalat Security Now by TWiT The CyberWire by N2K Network Risky Business by Patrick Gray	Free

CONCLUSION

Embrace Your Journey

In cybersecurity, there's no one-size-fits-all, and that's what makes this field so exciting. Sometimes, I wish I'd stumbled into cyber earlier, back in high school or during my Texas A&M days, so I could quickly change my major (again). But you know what? I am grateful for how I found my way here and when I did. If I were to rewind my journey into cyber, I wouldn't change a thing. Surprisingly, my degree in Political Science has been a hidden asset, offering a different perspective from the typical tech whiz who's been coding since birth.

My journey into cybersecurity taught me the power of curiosity as I bombarded my husband and his friends with a lot of questions to ensure I was making the right move for myself. What solidified my interest in cyber was taking Jason Dion's Security+ course and I have been in love with my field ever since. In retrospect, it's funny I didn't even consider the earning potential before diving in, just desperately searching for my life's path after losing interest in law school.

I urge my readers to dig deep, research, reflect, and take the self-assessment provided in this guide. Finding a cyber role that syncs with your lifestyle, and passion, and where you can truly make an impact can make a lot of difference.

Everybody's journey is unique. Whether you are a seasoned IT professional looking to pivot in a focused cyber role, or you're coming from a different field, you belong here. Embrace your path- it's what makes this journey in cybersecurity so wonderfully diverse.

- JEANIFFER