CAREERS CHECKLIST

CYBERSECURITY, PRIVACY, AND DATA PROTECTION

nalp We advance law careers

Download this resource at
www.nalp.org/careerservices

Introduction

Careers in cybersecurity, privacy, and data protection offer a range of opportunities and are described as JD Advantage jobs, meaning that a law degree is considered highly advantageous but not always required for hiring purposes. Law school graduates are highly valued in cybersecurity, privacy, and data protection fields because they possess technical experience as well as strong research, analytical, and communication skills. Cybersecurity, privacy, and data protection positions exist in all industries including banking and finance, insurance, medical, retail and hospitality, and education to name a few.

This checklist outlines key questions you should ask yourself as you pursue careers in cybersecurity, privacy, or data protection.

Definitions

Let's begin by defining cybersecurity, privacy, and data protection, as each is unique to itself albeit connected to one another.

- ✓ **Cybersecurity** is the process of and the protection against criminal or unauthorized use of electronic data. Online retailers are required to protect consumers' payment information from hackers and other nefarious individuals and organizations.
- ✓ **Privacy** is typically a regulation or statute that protects a person's right to be left alone as well as how an individual's financial, medical, and other personal information may be collected, stored, and released.
- ✓ **Data protection** is the safeguarding of important information from corruption, compromise, or loss. For example, when your doctor's office has a duty to safeguard data regarding your medical history, insurance, and payment information.

Is cybersecurity, privacy, or data protection for you?

It depends. National employment statistics for recent law school graduates clearly demonstrate that JD Advantage careers continue to grow in popularity. The key is knowing if the fit is right for you. Shifting from a traditional lawyer position into an exciting, fast-paced role of business advising can be a positive move and offer a unique opportunity if it aligns with your strengths, interests, and values. Your legal training is valuable and complements the other competencies required of cybersecurity, privacy, and data protection professionals.

Keep in mind that the fields of cybersecurity, data privacy, and data protection are new frontiers. The laws and regulations that exist today did not exist a few years ago. Individuals who work in the areas of cybersecurity, privacy, and data protection need to be innovative, creative, patient, and persuasive. You will literally be writing the laws that will govern the future of an ever-evolving tech world.

If you are exploring cybersecurity, privacy, or data protection options, schedule a meeting with your career services office and speak with an advisor. Your school may have specific resources and contacts that will help you make a decision that's right for you.

What skills are most valuable to cybersecurity, privacy, and data protection professionals?

Technology skills

Do you have experience with computers? Coding? Do you have a bachelor's degree in Information Technology, Data Forensics, or Computer Engineering? Degrees and technical experience offer insight and skills that coupled with a JD move a candidate forward in cybersecurity, privacy, and data protection positions.

Problem-solving skills

Are you able to spot the forest through the trees? Do you operate well in the gray? Are you able to assess all of the pros and cons surrounding an issue? What's truly important and what's less important to help others make good decisions that are in the best interests of the business? Are you able to challenge existing processes or products?

Written Communication skills

Do you have strong technical writing skills? Do you have the ability to convey your research and provide guidance that protects the company? Can you write clearly and concisely? Are the i's dotted and the t's crossed? Is the grammar correct and are all the pages accounted for? Did you use spellcheck and proofread for typographical, formatting, and factual errors?

Oral Communication skills

Are you able to communicate with different kinds of people, particularly IT staff and management, executives, and legislators? Can you "talk techie"? Can you speak with authority and translate complex regulatory issues into plain English?

Investigatory skills

You need to dig deep and leave no stone unturned. Are you the type of person who truly enjoys researching until you are satisfied that you have exhausted all avenues of inquiry?

Research and analytical skills

Do you possess strong research and analytical skills with an emphasis on analyzing laws and regulations to insure that a consumer or a company's interests are legally protected?

What courses should you take?

- ✓ **Begin with courses in Privacy Law, Legal Technology, Cybercrime, or Internet Law courses.** Courses that deal with privacy issues or technology are valued. Find the law school courses the have these types of components.
- ✓ **Enroll in specific courses in compliance, cybersecurity, privacy issues, consumer protection, Internet law, legislation, or administrative law.** Speak to your law school's registrar to learn what courses will be offered in the next two to three semesters. Law schools plan ahead and it's helpful for you to understand what will be offered – and what may be offered next semester and won't be offered again until after you graduate!
- ✓ **Take courses at another law school.** If your school does not offer specialized and relevant courses, are you able to take such courses online or at another school nearby? Again, check with your registrar to learn about taking courses at other schools.
- ✓ **Pursue an LL.M. in Cyber Law, Technology, or the like.** Some LL.M. programs will offer a more refined look at topics related to cybersecurity, privacy, and data protection. Consider LL.M. programs from law schools outside the United States.
- ✓ **Find out if your school offers a Master's in Legal Studies (MLS) degree or certificate courses in cybersecurity, privacy, or data protection.** Sometimes there are great courses hiding in plain view at your law school, but you need to investigate. Some law schools now offer MLS degrees specifically in the area of privacy or cybersecurity. If this is the case, ask your faculty advisor and registrar for a list of offerings and learn if you can cross-register for courses that pertain to cybersecurity, privacy, and data protection.
- ✓ **Explore business school offerings.** If your law school is part of a larger university and has a business school, you may want to explore if the business school offers compliance, cybersecurity, privacy, and data protection courses that would enhance your knowledge and build your resume.

What certifications should you acquire?

Earning a certification and adding this credential to your resume can help set you apart from other candidates. Consider the following certifications as a starting point in your cybersecurity, privacy, and data protection career exploration:

- ✓ **IAPP** (iapp.org), the International Association of Privacy Professionals, is the largest and most comprehensive global information privacy community and resource. Founded in 2000, the IAPP is a not-for-profit organization that helps define, support and improve the privacy profession globally. IAPP offers several privacy law certifications to demonstrate your command of relevant laws and regulations.

- ✓ **CompTIA Cybersecurity Analyst (CySA+)** Certification is an international, vendor-neutral cybersecurity certification that applies behavioral analytics to improve the overall state of IT security. CySA+ validates critical knowledge and skills that are required to prevent, detect and combat cybersecurity threats.

- ✓ **Certified Cyber Forensics Professional (CCFP)** "CCFP certification indicates expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete, and reliable digital evidence admissible in a court of law. It also indicates the ability to apply forensics to other information security disciplines, such as e-discovery, malware analysis, or incident response."

What's the best work experience?

There are many avenues into cybersecurity, privacy, and data protection, and it depends on many factors such as whether or not the role is entry-level, mid-level, or senior. The good news is that many work experiences are viewed favorably for such roles, including law firms, government agencies, and in-house legal departments. It all goes back to your skills, academic courses, and certifications.

If possible, get experience in the industry to learn the business issues and regulatory challenges. For instance, prior work in banking and finance can translate into in-depth knowledge of the protection of financial data or experience in cloud management can assist with cybersecurity regulations.

In your final year of law school, you may still have time to gain some work experience, however brief, to make your resume stand out. Consider a short stint (paid, unpaid, volunteer, or internship for academic credit) to get yourself in the door and to learn about a target industry with an eye toward cybersecurity, privacy, or data protection.

It is equally important to highlight relevant pre-law school experience. Do not assume that prior experience, at any level, will be of limited use to a prospective employer. Such experience in areas like technology, coding, forensics, lobbying, and public policy coupled with legal experience in drafting regulations, white papers, or other industry-specific experience will be of great use.

Cultivate Your Network

Networking is an important aspect of any job search and jobs in cybersecurity, data protection, and privacy are no exception. In addition to developing a strong resume, you should cultivate relationships with cybersecurity, privacy, and data protection professionals to gain inside knowledge about what a particular business is hiring for. Here are some ways to build your network to maximize opportunities in cybersecurity, privacy, and data protection:

Start with your law school career services office.

Ask an advisor to help identify graduates who work in cybersecurity, privacy, or data protection and schedule informational interviews with alumni.

Ask faculty members to connect you with cybersecurity, privacy, and data protection experts.

Adjunct professors who teach cybersecurity, privacy law, or data protection courses may have very strong networks in the area. Ask for assistance making these connections.

Attend cybersecurity, privacy, or data protection programs at your law school.

Attend programs featuring cybersecurity, privacy, and data protection professionals sponsored by your law school career services office or student groups. These types of programs present golden opportunities to hear first-hand about entry into cybersecurity, privacy, and data protection careers and to connect with the speakers who are often alumni and inclined to help.

Utilize alumni directories (law school and undergraduate) that enable you to identify graduates who are working in cybersecurity, privacy, and data protection fields.

You can use a keyword search or search using titles such as Chief Privacy Officer, Government Privacy Analyst, Cybersecurity Trainer, Vulnerability Analyst, Threat Intelligence Analyst, or Security Engineer, to guide you.

Seek out bar associations specific committees for lawyers working in cybersecurity, privacy, and data protection.

For instance, the American Bar Association Cybersecurity, Privacy, & Data Protection Committee attracts lawyers with cybersecurity, privacy, and data protection-related jobs and holds panel discussions and other forums for lawyers to network and learn throughout the year.

Join professional associations such as the International Association of Privacy Professionals (IAPP) or the Information Systems Security Association (ISSA).

Such associations offer student memberships, access to certification, conferences and trainings, and many opportunities for networking and building relationships.

How should you present your credentials on your resume and cover letter?

- ✓ **Highlight transferable legal skills** such as investigations, research, drafting, and analysis.
- ✓ **Choose your words carefully.** Some companies scan resumes and then search by keyword, so be sure to craft your resume to use words that mimic a job posting's language.
- ✓ **Emphasize experience with technology, forensics, regulations, lobbying, as well as prior professional experience,** particularly back-office operations in the industry you are focusing on. These types of skills or experiences are typically not listed on traditional law resumes, but you need to think expansively about the range of experiences and skills you've acquired outside of traditional law practice.
- ✓ **List specific courses that are privacy or security-oriented** such as Cybersecurity and Privacy Law, Health Law Regulations, etc.
- ✓ **List relevant certifications prominently on your resume.** This section may also include relevant legal certifications and licenses.

What is a career path like in cybersecurity, privacy, and data protection?

The trajectory of a cybersecurity, privacy, or data protection career depends on the industry, whether it is banking, hospitals, higher education, or corporations. Law graduates who enter the cybersecurity, privacy, or data protection fields can find lateral opportunities with an employer, using their legal training to add value, rising to management or supervisory roles. There may also be opportunities to move between employers, entering business consulting with one's area of expertise, or even moving into a law firm if one's expertise is valued as an asset in advising clients. While some individuals move between law and business seamlessly, it's difficult to stay current in two professions simultaneously so be sure you are making a well-reasoned decision when you choose cybersecurity, privacy, or data protection as it's unusual to move to a law firm. Staying involved with local bar associations and maintaining a strong network of business contacts helps to keep your options open.

Other Resources

- ✓ ***Data Protection Practice*** by Richard L. Hermann offers in-depth advice, websites, and resources.
- ✓ ***Privacy, Law Enforcement, and National Security*** by Daniel J. Solove and Paul M. Schwartz offers insight into cases related to government surveillance and national security.
- ✓ ***Cybersecurity Law*** by Jeff Kosseff offers an "in-depth analysis of U.S. and international laws that apply to data security, data breaches, sensitive information safeguarding, law enforcement surveillance, cybercriminal combat, privacy, and many other cybersecurity issues."
- ✓ ***The New What Can You Do with a Law Degree?*** by Dr. Larry Richard and Tanya Hanson offers a step-by-step guide for law students or lawyers who are contemplating a JD advantage career.
- ✓ Explore jobs on LinkedIn (keywords "**cybersecurity**"; "**privacy**"; or "**data protection**") and Indeed.com to gain more familiarity with openings in your area. You can create a saved search that will automatically generate a list of openings daily.

Getting Started

Decide if the world of cybersecurity, privacy, and data protection is right for you.

Conduct research and explore through books, articles, websites, informational interviews, and career counseling.

Plan your courses with an eye toward positions in cybersecurity, privacy, or data protection.

If you are still in law school, take courses that deal with cybersecurity, privacy, or data protection issues so you can expand your knowledge and get to know professors who may assist you in your career exploration. If you attend a law school that is part of a larger university, ask about courses offered through the business school or IT programs that focus on cybersecurity, privacy, or data protection issues. Some law schools now offer masters programs (non-JD) that teach cybersecurity, privacy, or data protection and those courses may also be available to you as a JD student.

Draft a resume with a cybersecurity, privacy, or data protection position in mind.

There's more than one way to draft a resume! Cybersecurity, privacy, or data protection resumes look different from traditional law school resumes. Ask your career services office for examples and revise your resume to conform to employers seeking to fill cybersecurity, privacy, or data protection positions. Consider listing relevant courses that you have taken or plan to take to highlight your commitment to cybersecurity, privacy, or data protection work.

Build your network.

Engage in informational interviews with alumni, faculty, and others who are working in cybersecurity, privacy, or data protection. These individuals can help answer your questions, identify job opportunities, and coach you about how to succeed with applications and in interviews. Your career services office can help you identify alumni who work in cybersecurity, privacy, or data protection. Like any career exploration, you need to cultivate relationships and find allies to assist you.

Use LinkedIn and other search engines effectively.

Both LinkedIn and Indeed.com are good places to start exploring job postings in the cybersecurity, privacy, or data protection fields (with the understanding that it's equally important to build your network). You can set up job search alerts on each site that will identify when relevant jobs that fit your profile are listed.

Determine if you need a certification in your area of interest.

Earning a certification as a Cyber Security Analyst or Data Forensics Specialist can help distinguish you from the competition. Conduct your research and determine if you can tick off a certification while in law school to boost your candidacy.

Understand the career timeline for positions in cybersecurity, privacy, or data protection.

Unlike most legal jobs that begin with a full-time, long-term offer, many employers may initiate the hiring process with full-time, short-term contract positions. Candidates are paid an hourly rate and trained in a particular cybersecurity, privacy, or data protection function for an assignment that may last several months. At the end of the contract period, a few candidates are asked to remain and are trained further and ultimately receive full-time, long-term offers with salaries. Understanding the hiring practices in a particular cybersecurity, privacy, or data protection field will make you a more sophisticated job applicant and enable you to succeed in the long-term. ■

National Association for Law Placement (NALP)
1220 19th Street NW, Suite 401
Washington, DC 20036-2405
Phone: (202) 835-1001 | Fax: (202) 835-1112
www.nalp.org