Building the next generation of security and privacy professionals

By IAPP Managing Director, D.C., Cobun Zweifel-Keegan, CIPP/US, CIPM, and IAPP Westin Fellow Anokhy Desai, CIPP/US, CIPT
Contents

EXECUTIVE SUMMARY .............................................................. 3

THE GROWTH OF DATA PROFESSIONS ..................................... 5

THE ROLES OF PRIVACY AND CYBERSECURITY PROFESSIONALS ... 7

COMMON CHALLENGES IN THE DATA STEWARDSHIP PROFESSIONS ................................................................. 9
- Workforce gaps ........................................................................ 9
- Management buy-in and limited resources ............................. 10
- Evolving best practices: the need to stay nimble .................... 11

SECURITY OF PRIVACY AND PRIVACY OF SECURITY .............. 12

CONCLUSION: A GROWING SYMBIOSIS .................................... 13

CONTACT ..................................................................................... 14
Executive Summary

Organizational practices in the digital age are inevitably linked to the processing of data, and built upon the systems that support these efforts. Collectively, cybersecurity and privacy professionals are responsible for guiding and implementing organizational decisions that ensure data is collected, processed, protected and shared consistent with evolving norms. As technologies, threats, and regulations continue to shift, privacy and security functions benefit from an increased awareness of each other's activities, priorities and goals.

- **Privacy and cybersecurity have increasing synergy:** As privacy and cybersecurity functions mature and businesses become more reliant on data, a blend of privacy and cybersecurity capabilities is needed across business functions. Organizations that encourage cybersecurity and privacy professionals to work closely together can leverage synergies in roles to improve cyber and privacy postures, reduce risk and gain flexibility and efficiency.

- **Collaboration helps address resource challenges:** The demand for privacy and cybersecurity professionals has never been greater. Working together closely can provide a competitive and cost advantage, while alleviating some resource pressures.

*Case studies continue to proliferate showing why this mutual understanding is essential. Crossfunctional training and communication will be ever more necessary in building the next generation of data stewards.*
To leverage the benefits, knowledge sharing is key: Privacy and cybersecurity professionals can embrace knowledge-sharing and crossfunctional training to more efficiently protect the data collected and used by their organizations. Finding community across the aisle can help in building organizational support and management buy-in for updated processes that would require using part of a shared budget. A symbiotic relationship also helps the organization stay nimble as regulations continue to evolve. In addition, the privacy profession can learn from the skills gap challenges cybersecurity faces, as illuminated through a 2022 workforce study conducted by (ISC)². Similarly, security professionals must understand the contours of privacy risk to ensure properly tailored operations and avoid inadvertently violating privacy norms. Case studies continue to proliferate showing why this mutual understanding is essential. Crossfunctional training and communication will be ever more necessary in building the next generation of data stewards.
The growth of data professions

The digital age has brought with it the ubiquity of data. Ubiquitous data, of all kinds, has necessitated the spread of organizational roles that manage, organize and safeguard this data.

At the most basic level, cybersecurity is concerned with ensuring the right mix of confidentiality, availability and integrity of data and systems. The field of privacy, also known as data protection, is concerned with ensuring the trustworthy management of personal information, as it is collected, used, retained, shared and disposed. Other related fields, from data governance to data ethics, concern themselves more broadly with the management of information through a variety of lenses.

Broadly speaking, such stewards of data generally interact across two common narratives:

- **Data as an asset**: Organizations strive to utilize the right blend of data elements to support their strategic goals, deliver enhanced customer experience, and unlock new opportunities for insight-based decision-making, innovation and value creation.

- **Data as a liability**: Organizations must respond to an ever-changing global landscape where evolving legal norms, nefarious threat actors and customer expectations drive them to implement complex measures to address their data risks.

Together, these roles serve a fundamental component of the success of any organization in the digital age. Though the fields of privacy and cybersecurity differ, they are both characterized by a professionalized workforce.

**FIGURE 1**: Effective data stewardship requires harmony and understanding between the privacy and cybersecurity fields
What makes a profession? Many hundreds of years ago, the rise of labor specialization brought with it a need for organized professions. What began with artisan and merchant guilds matured in the industrial age into structured and organized skillsets, which grew to be increasingly ordered and regulated. In their book “The Future of the Professions,” Richard and Daniel Susskind trace back the history of the concept of professions, observing that an array of jobs, from dentistry to management consulting, “are worthy of this label.” They note modern professions (1) have specialist knowledge, (2) admit members based on credentials, (3) have regulated activities and (4) are bound by a common set of values. The dictionary definition of “profession” echoes this focus on credentials; a profession is a “paid occupation, especially one that involves prolonged training and a formal qualification.” Based on these criteria, the privacy and cybersecurity fields have reached the baseline status of professions.

Even as the professionalization of both roles continues, they are becoming more intertwined. While they require different knowledge bases, privacy and security go hand in hand. Effective data privacy is impossible without robust security measures. And a cybersecurity department that is not aware of the special risks of personal data is flying blind. Now, more than ever, organizations should encourage their privacy and cybersecurity professionals to acquaint themselves with their counterparts’ roles, responsibilities and goals, especially as the overlap in skills, knowledge and need continues to grow.

**FIGURE 2:** Balancing the importance of IT experience, education and certifications for entry- and mid-level positions in the cybersecurity profession

- **Have IT experience**: 50% Nice to have, 47% Critical, 3% Not necessary
- **Have educational background in security**: 47% Nice to have, 47% Critical, 6% Not necessary
- **Hold IT/security certifications**: 45% Nice to have, 51% Critical, 4% Not necessary

Adapted from (ISC)^2 2022 Cybersecurity Hiring Managers Guide.
The roles of privacy and cybersecurity professionals

Just five years ago, 35,000 individuals were qualified as privacy professionals, holding roles as lawyers, technologists, and administrators in both the public and private sectors. Now, the International Association of Privacy Professionals boasts more than 75,000 privacy professional members in more than 150 countries and is the only established organization providing ANSI-accredited certifications for individuals seeking to practice in the field.

Reminiscent of the early days of cybersecurity, individuals in these privacy roles who did not graduate with a degree in or adjacent to privacy often volunteered for emerging roles managing data policies and procedures. Over time, these privacy roles began to reflect a discrete body of knowledge passed down within and between institutions, and through the profession itself.

Today, this evolving body of knowledge is reflected in professional certifications like the Certified Information Privacy Professional for Asia, Canada, Europe, and the U.S., the Certified Information Privacy Manager, and the Certified Information Privacy Technologist. The spectrum of privacy certifications reflects the interdisciplinary nature of the profession, with roles held by lawyers, technologists and those with other backgrounds still vastly outnumbering those with degrees focused on data protection. With new privacy regulations emerging at a breakneck pace, the profession continues to grow exponentially.

FIGURE 3: Pathways to cybersecurity careers

Workforce 2022 Participants Pathways to Cybersecurity Careers

- Started in IT then moved to cybersecurity: 69% - 70%
- Started in another field then moved to cybersecurity: 16%
- Pursued education in cybersecurity or related field then got my first job in cybersecurity: 19%
- Explored cybersecurity concepts on my own and was recruited for a job in cybersecurity: 3%

Adapted from (ISC)² 2022 Cybersecurity Workforce Study.
In the early 2000s, the cybersecurity profession saw a similar growth trajectory and expansion of roles. In the decades that have followed, positions continue to be increasingly specialized. In its 2022 (ISC)² Cybersecurity Workforce Study, the professional association for cybersecurity, (ISC)², estimated more than 4.66 million security professionals globally, historically with most professionals starting in information technology and moving to cybersecurity. The respondents held roles across the professional spectrum, from entry-level technical staff to C-suite positions, and reported holding a variety of certifications ranging from CompTIA’s A+ to the CISSP. The varied range of specialties and experience levels necessary not just to pass but to take certain security certifications reflects on the maturity of the profession.

Many cybersecurity and privacy professionals report that their roles overlap significantly with their counterparts, even if they do not hold certifications or trainings in other data governance fields. As the privacy profession continues to mature, and cross-domain teamwork becomes more necessary, it is likely to become increasingly common to see privacy and cybersecurity professionals hold certifications in both fields.

**FIGURE 4: Distribution of job titles in privacy and cybersecurity roles**

![Pie charts showing the distribution of job titles in privacy and cybersecurity roles.](image)

Adapted from the IAPP 2021 Privacy Professionals Salary Survey, pg. 10, and (ISC)² 2022 Cybersecurity Workforce Study.
Common challenges in the data stewardship professions

Workforce gaps

(ISC)²’s research shows the cybersecurity skills gap stands at 3.4 million globally. Fifty-six percent of participants in the 2022 (ISC)² Workforce Study reported that a cybersecurity staffing shortage was putting their organizations at risk, despite the influx of 464,000 new hires in the field. The gap between the global demand for cybersecurity professionals is continuing to outpace the supply, with the highest need in investigation, security provisioning, protection, analysis, governance and operations.

The 2022 (ISC)² Workforce Study showed this workforce gap leads to dramatic consequences, including misconfigured systems, lack of time for proper risk assessment and management, oversights in process and procedure, slower patches to critical systems, not enough time to train cybersecurity staff, misconfigured systems, and rushed deployments.

There are fewer data points about the lived experience of the workforce gap in privacy, with the maturity of the cybersecurity profession nearly a decade in the lead.

Nevertheless, it is apparent that the workforce is struggling to keep up with the demand for privacy professionals.

FIGURE 5: Real consequences of staff shortage

- 48% Not enough time for proper risk assessment and management
- 35% Misconfigured systems
- 43% Oversights in process and procedure
- 32% Not enough resources to adequately train our staff
- 39% Slow to patch critical systems
- 30% Rushed deployments
- 38% Not enough time to adequately train each cybersecurity team member

Adapted from (ISC)² 2022 Workforce Study.
“It’s small wonder the global privacy profession continues to see near exponential growth as it adapts to new compliance challenges, seemingly every week,” said IAPP President and CEO, J. Trevor Hughes, CIPP.

In Europe alone, the IAPP estimated in 2019 that 500,000 organizations had registered data protection officers. IAPP’s annual salary survey also reflects that demand is outpacing supply. “It’s small wonder the global privacy profession continues to see near exponential growth as it adapts to new compliance challenges, seemingly every week,” said IAPP President and CEO, J. Trevor Hughes, CIPP. Already 130 countries have data protection laws on the books. As best practices mature and compliance obligations spread around the world, the practice of data privacy will continue to proliferate.

Between the need to effectively defend and manage organizations’ critical assets — people, customers, technology, information, facilities and equipment, systems, and processes — and to maintain compliance with the growing list of different states’ and sectors’ privacy and security requirements, estimates show that the global cybersecurity and privacy workforce needs to see a collective increase of 74% in order to meet current demand.

- Management buy-in and limited resources

In addition to the workforce gap, another shared challenge among cybersecurity and privacy professionals is the ever-present balance between obtaining buy-in from management and competing with other organizational priorities for limited resources. Across the marketplace, data stewards can face pushback on solutions or policy implementations. Often, they reside in departments or roles that are viewed as overhead. Security and privacy personnel who handle data have an important role in their organization, not just as stewards of data but also as shepherds of organizational reputation. Yet decisionmakers can view compliance — and even consumer trust — as low-priority cost centers. Therefore, it is important for data professionals to get buy-in from relevant stakeholders early and often by demonstrating the essential nature of their work.

This does not mean only building relationships with leadership. Connecting across functions also allows cybersecurity and privacy professionals to get a better sense of how data management affects other departments, fits in the scope of their organization's goals, and brings added value. Cybersecurity and privacy professionals are hired for a reason and fulfill clear objectives for the health of their organization. Organizations that want to do right by their customers, employees and partners do not simply hire data stewards for the sake of meeting a compliance checklist item. They understand it is their role to promote the most effective data handling and privacy practices, increase consumer trust and even better align the company with its strategy.

To help achieve advance mutual objectives, teamwork and cross-training across the privacy-security divide is becoming more important. Security and privacy professionals should be familiar with each other’s roles in the organization, and even with some of their job duties. Organizational leaders should recognize this reality when investing in these roles. If job duties are shared, it is important to determine early on whether a budget is also shared. A limited
Each regulation adds its own on privacy. Some of the most recent regulations represent opening salvos in an ongoing shift from a privacy regime focused on notice and choice toward one rooted in principles like data minimization and use specification.

Similarly, as cyberattack vectors shift and the threat landscape evolves, so do reasonable security standards. Cybersecurity requirements are updated regularly in controls as new responses are needed to address unprecedented attacks. As the expectation of reasonable security changes with every iteration of encryption protocols, freshly uncovered vulnerability and new breach, so too does what constitutes effective best practices in security.

Cybersecurity and privacy professionals embody the difficult balance of needing to keep up with and advise their organizations on how to proceed with best practices. This may be why we continue to see increases in crossover of privacy and security guidance, as shown by the new ISO-27701 controls. Similarly, the U.S. National Institute of Standards and Technology recently underwent its own evolution with the release of the NIST SP 800-53, Rev. 5 controls for security and privacy. The updated controls "represents a multi-year effort to develop the next generation of security and privacy controls needed to strengthen and support the Federal Government and every sector of critical infrastructure." These controls reflect more recent threat vectors, as evidenced by the addition of a supply chain management control family and the improved descriptions of content relationships between requirements and controls, and more notably, security and privacy controls.

Evolving best practices: The need to stay nimble

Best practices evolve as new data-intensive technologies spread, new regulations pass and consumer expectations shift. It should come as no surprise in this “era of the cloud” and connected devices, with ubiquitous sensors and data flows proliferating that a nimble approach to data stewardship is needed. New risks lead to new rules. And updated rules lead to new norms for how best to ensure responsible data governance.

In the last few years, we have seen a proliferation of privacy laws across the world, from China to California. They have built on the concepts of the EU General Data Protection Regulation, including new requirements and specifications. Though trends and patterns continue to emerge, budget spread across multiple departments can lead to competition over resources by individuals whose goals overlap.

A board of directors and company executives will especially support a data steward’s case for better privacy when framed within the context of risk management. Risks of data exposure, loss of trust, and regulator scrutiny are pressing organizational concerns that are all heightened when personal data is involved. Those implementing privacy updates will similarly need reminders that better security practices directly lead to better privacy outcomes. A more robust risk management plan means having an organized response to a cybersecurity breach in which private information is exfiltrated. It also means staying nimble in the fast-paced world of data.
Security of privacy and privacy of security

To meet industry standards, data security professionals must incorporate privacy best practices into their knowledge base — or work closely with privacy professionals to ensure that norms are not violated.

The U.S. Federal Trade Commission’s recent enforcement action against Twitter illustrates the importance of implementing practices like purpose limitations into security processes. Twitter sought to improve user security by enabling multifactor authentication. However, according to the FTC complaint, although users were prompted to provide their email addresses or phone numbers for security purposes, Twitter also used this contact information to deliver targeted ads to its users. Here, better security practices did not automatically mean better privacy outcomes. Even as multifactor authentication was successfully promoted to better safeguard user security, users lost privacy when that data was given to advertisers without their knowledge or consent.

Incorporating privacy fundamentals into data security processes can also improve outcomes. Cybersecurity company Critical Insights reported breaches in the health care sector hit an all-time high in 2021, rising from 14 million affected individuals in 2018 to a whopping 45 million. These breaches not only indicate the lagging state of security across the sector during a critical period, but they also exposed a record number of patients’ protected health information. In the health care context, a recent McKinsey report stressed the importance of the EU GDPR as a new baseline for health data in a world where not all health data is protected under industry-specific regulations. It notes the EU GDPR ensures data protection measures are in place to limit practices that may not inherently raise cyber risk, such as health tracking by employers, the collection of health data that is not essential to a business need, and expanded uses of legally collected data. Privacy serves an important role in helping security professionals understand why some data may pose enhanced risks and deserve enhanced protections.

Conversely, the security of personal information and the systems that store and transmit this data has always been considered one of the fundamental principles of privacy. Privacy professionals understand that practices like controlling the access and use of personal information are impossible without industry-standard security protections. At a basic level, a company without proper technical protocols like encrypted passwords faces a higher risk of a data breach turning into a privacy breach.

“The intersection of security and privacy has been evident for years,” said (ISC)² CEO Clar Rosso. “This is why it is so critical that privacy and cybersecurity pros work collaboratively to ensure strong and effective data stewardship.” Those professionals who can speak the language of both privacy and security have a crucial role to play in organizations. Without implementing proper security protocols, privacy professionals are hobbled. And without an understanding of privacy fundamentals, even the best security proves useless.
Conclusion: A growing symbiosis

Even as cybersecurity continues to see exponential growth, the pathways to careers in security are diverse. While having an IT education and work background remains the single most common route taken, with 63% of the (ISC)² study participants indicating this as their entry into cybersecurity, this track has given way to a variety of other entry points in recent years.

- Just over one-third of cybersecurity professionals got their start outside of IT.
- 17% transitioned from unrelated career fields.
- 15% gained access through cybersecurity education.
- 15% explored cybersecurity concepts individually.

It is through the role of the centralized profession — through trainings, certifications, accreditations and knowledge sharing — that these diverse career paths are harmonized into unified fields.

The privacy profession has followed close behind these trends. Individuals across a range of backgrounds — law, policy, professional services, technology, advertising, human resources — hold privacy roles and identify as part of the privacy profession. Cybersecurity professionals, too, increasingly identify as privacy professionals. The growing field of data security, concerned with the protection of personal data, continues to emerge as a core role of proper data stewardship.

It is because of this growing overlap that those in privacy and security roles who manage, handle, or oversee the collection and use of data in their organizations, should embrace the merging of workforce roles and skills. Not only are privacy and security professionals overlapping more in their job duties, but they are also faced with circumstances that would best be managed with a deeper understanding of their counterparts’ industry.

Teams should consider incorporating actionable objectives to keep up with this trend, from incorporating privacy and security concepts into the development lifecycle, to cross-training teams as a preventive measure against security features that worsen privacy outcomes. Regardless of method, cybersecurity and privacy professions will greatly benefit from the growing group of cybersecurity and privacy professionals in the years to come.

The IAPP and (ISC)² understand the importance of these synergies. This paper represents the first step in an ongoing collaborative effort to ensure organizations benefit from cross-functional, nimble and well-resourced professionals in both fields. Moving forward, we will continue to collaborate across targeted projects to help deliver insights and value to our members.

“The intersection of security and privacy has been evident for years,” said (ISC)² CEO Clar Rosso. “This is why it is so critical that privacy and cybersecurity pros work collaboratively to ensure strong and effective data stewardship.”
Published October, 2022.

The IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2022 International Association of Privacy Professionals. All rights reserved.