The Age of the Cyberpro

Prepared by

The Ohio State University
Michael E. Moritz College of Law
Program on Data and Governance[1]

Professor Dennis Hirsch, Faculty Director
Keir Lamont, Program Manager

The siloed data governance professions of today will not be able to meet organizations' data risk management needs of tomorrow. Changes in the digital society and the laws that govern it will require solutions that draw simultaneously from the cybersecurity, privacy and information technology governance fields. The professionals best equipped to deliver these solutions will have hybridized skills and fluency across these various domains, though they may specialize in one or the other. These cyberprofessionals – "cyberpros," for short – will be able to meet the needs of their organizations and of society at large far more effectively than those who remain limited to their respective silos. This report explains why this is so. It begins by describing why the members of the cybersecurity and privacy professions will perform better when they become more conversant with each other's fields. It then turns to the information technology governance profession and explains why it needs to become more familiar with the cybersecurity and privacy professions, and they with it. It concludes that future of the data governance professions lies in cross-domain fluency and collaboration. We are entering the age of the cyberpro.

[1] This report was funded by a grant from the International Association of Privacy Professionals.

Cross Fluency Between the Cybersecurity and Privacy Professions

Traditionally, the cybersecurity and privacy professions have focused on different domains and brought distinct skill sets to their roles. Cybersecurity professionals have focused on technologies, policies and procedures to ensure that information assets and technologies are adequately protected. They bring technological and management expertise to their tasks, but are less apt to employ legal or humanities-based approaches. Privacy professionals are different. They concern themselves with the collection, use and sharing of personal information and the social and legal norms that govern these activities. Most are fluent in legal and regulatory matters and bring a humanities or social science background to their work but are less conversant in matters of technology.

Cybersecurity professionals who draw more on the privacy field and its legal and humanistic modes of analysis will better be able to achieve security goals for a number of reasons. First, a cybersecurity professional who can determine which personal data is more sensitive and which is less so — a staple of the privacy field — will be able to calibrate access controls to the sensitivity of the data rather than applying a maximalist approach to all personal information, and so will be able to achieve security in more cost-effective ways. Second, cybersecurity professionals who understand privacy laws will be able to design security controls that stay within these laws' important boundaries. Third, those who have studied users' expectations of privacy will be able to design security measures that are not perceived as intrusive and will not "creep out" customers or employees in ways that will damage organizations' bonds of trust with these key stakeholders. Finally, today's cybersecurity professionals need greater familiarity with the Federal Trade Commission, a regulatory entity that privacy professionals have worked with for decades. The FTC has begun to assert itself more

strongly in the security area, maintaining that unduly lax security measures are "unfair" to consumers and may violate Section 5 of the FTC Act. Cybersecurity professionals learning to engage with this regulatory agency could draw profitably on the privacy field's longstanding experience with it.

Cybersecurity professionals could also become more effective by integrating more of the social science- and humanities-based approaches of their privacy counterparts. For example, researchers at Carnegie Mellon have shown that security policies that require users frequently to change their passwords often cause them to select shorter, weaker passwords and to change them in minor, predictable ways.[2] To avoid such pitfalls, security professionals need to account more for human nature and human behavior, topics on which the humanities and social sciences focus. As a recent CPO Magazine article explained, cybersecurity, a technology-focused area, and data privacy, a law and humanities-based one, "are increasingly closely related." The most effective professionals in these two areas will be those who incorporate the other's way of approaching problems.[3]

Just as cybersecurity professionals will gain from greater familiarity with the privacy field, so privacy professionals will benefit from engaging more with cybersecurity and technology. For example, privacy professionals who participate in the purchase or design of access control systems can better ensure that employees are able only to interface with the data that is relevant to their business needs. This can prevent employees from taking data that was collected for one purpose and using it for another, incompatible purpose, and so help organizations to comply with the "purpose limitation

[2] See e.g. https://www.ece.cmu.edu/~lbauer/papers/2016/tissec2016-password-policies.pdf
[3] https://www.cpomagazine.com/2016/09/21/rise-chief-security-privacy-officer/

principle," a key element of privacy compliance. Privacy professionals engaged with the design of security systems can also provide input into the type of access that each employee should have (read-only, edit, share) and so better prevent privacy-compromising events like employee spying on celebrities, politicians or ex-spouses.[4]

Privacy professionals will also benefit by becoming more conversant with technology. For example, those who understand de-identification and re-identification will be much better able to explain to their organization and to regulators whether particular data constitute personally identifiable information (PII) and so are covered by privacy laws. Greater technical knowledge will further allow them to identify privacy enhancing technologies such as encryption or privacy-protective data mining (differential privacy), explain how they work, and counsel their organizations on whether to invest in them. It will enable them to engage more productively in discussions about privacy depleting technologies such as "supercookies" or other tracking technologies and to assess the risks they pose to user privacy and to the organization. Finally, it will facilitate their working with their organization's engineers to employ technology for privacy purposes, such as the design of more user-friendly privacy notices. In each of these ways, increased technical expertise will make privacy professionals more effective. A 2017 article in the Harvard Business Review titled "Liberal Arts in the Digital Age" argues that the split between the STEM fields and the humanities is a "false dichotomy" and that success in the digital economy requires both. The benefits that privacy professionals achieve through expanding their technical

[4] http://www.nbcnews.com/tech/tech-news/uber-whistleblower-says-employees-used-company-systems-stalk-exes-celebs-n696371

knowledge, and that cybersecurity professionals gain by drawing more on the humanities and social sciences, illustrate this point.

Increased fluency across the two professions will also allow cybersecurity and privacy professionals to collaborate better and so to identify win-win scenarios that provide value to the organization. For example, data minimization, an important privacy tool, reduces an organization's store of data, makes it a less attractive target for adversaries, and so enhances cybersecurity. The privacy benefits alone may not warrant investment in particular data minimization measures. But combined with the cybersecurity benefits, they may significantly outweigh the costs. Organizations need to view such investments from the perspective of both fields simultaneously in order to be able to perceive and take advantage of such opportunities. The same might be said for cybersecurity measures such as limits on data sharing that have ancillary privacy benefits. Ultimately, cybersecurity and privacy professionals contribute to the same overall goal: ensuring that their organization handles personal information responsibly and so mitigates risk to itself and to others. They optimize this function best when they work together – something that is only possible when each becomes more conversant in the other's field.

Cross Fluency with the Information Technology Governance Field

Information technology governance professionals have overall responsibility for ensuring that the organization's information technology systems provide value and support its goals. They focus on ICT strategy, risk mitigation, management systems, and the physical, technological and management controls needed to achieve information assurance, among other important areas.

Information technology governance and cybersecurity professionals have, for some time, worked to acquaint themselves with each other's field and to collaborate with one another. IT governance professionals understand that data breaches and hostile systems intrusions, which can profoundly affect business operations and user trust, are strategic issues on which they need to focus. For their part, cybersecurity professionals know that security depends not just on technology, but also on effective systems design, administrative controls and assurance, areas in which IT governance professionals have expertise. Professionals in each field understand the benefits of learning more about the other and have begun to gain this knowledge.

The time has come for IT governance and privacy professionals to partner in a similar way. Recent technological and legal developments demand it. For many years, most organizations used personally identifiable information (PII) primarily in discrete departments such as human resources or marketing that are governed by specific privacy rules. The privacy professional mainly sought to ensure compliance with these rules. The rise of the cloud, big data analytics, the Internet of Things and associated technologies changes this dramatically. Today, many businesses and other organizations use personal data throughout their operations, products, and services. IBM CEO Ginni Rometty has argued that big data is the next great natural resource – the "new oil" – that will shape how companies learn about their consumers, as well as how they create and deliver value.[5]

In such a world, privacy professionals have to expand their role beyond traditional compliance. They need to make sure that the organization considers privacy at every point at which it utilizes personal information – which is to say, throughout the

[5] http://www.thedailybeast.com/ibm-ceo-rometty-says-big-data-is-the-next-great-natural-resource

organization – and that it institutes proper privacy protections at each such juncture. Privacy professionals use the term "privacy by design" to denote the notion that privacy should be a part of all product and process design choices. Successful implementation of privacy by design requires the ability to conceive of and implement management systems, assurance mechanisms, and administrative and technological controls around privacy. These are the very skills that IT governance professionals have honed over the years. Today's privacy professionals will benefit from partnering with their IT governance colleagues and drawing on their experience in these areas.

The spread of personal data throughout the business also has another effect: It greatly raises the stakes of failing to implement effective privacy controls. A major privacy snafu does not only pose a risk of regulatory penalties; it can also undermine users' and partners' trust in the organization, cause them to withhold personal data, and so have major negative repercussions for the business. This makes privacy a critical dimension of information risk management and very much the business of the IT governance professional.

The new technologies also change the landscape in another way. They pose personal information-related risks to organizations that go well beyond privacy. In one recent example, Facebook's "emotional contagion" study modified the Newsfeed algorithm to present some users with optimistic content and others with pessimistic content so as to determine whether this affected the users' own postings. When users learned of this, they felt manipulated by and angry at the company.[6] In another example, Amazon employed an algorithm to determine the neighborhoods in which it

[6] https://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/#8bbfe2939dc7

would offer its new same-day delivery service. A Bloomberg analysis revealed that, in six major cities, this led the company to exclude most predominantly African-American neighborhoods from the service.[7] Amazon had not anticipated this result and moved quickly to address it. Amazon and its customers would have been far better off it if the company had spotted it in advance.

These incidents centered on the use of personal information and so implicated privacy. But they also raised questions of bias, fairness, ethics and manipulation. Today's digital economy, with its ever-expanding use of personal data, raises many such issues. Successfully spotting and addressing them before an incident hurts people and makes the organization less trusted requires much more than formulaic check-the-box compliance centered on privacy statutes. It requires strategic thinking about the organization's core values, the development of audit systems to detect and address potential negative impacts, and the establishment of management controls to spot and evaluate ethical issues. This new frontier of data governance will favor companies whose privacy and IT governance professionals are talking to each other, are familiar with each other's field, and work together pro-actively to address risks and uphold corporate and societal values. Hybrid professionals will be best able to deliver this critical service.

Ongoing legal developments further drive demand for cyberpros with cross-domain fluency. The European Union's new General Data Protection Regulation (GDPR) – the most significant new privacy law in a generation – becomes effective May 25, 2018 and will impact any American company that uses European citizens' personal data. The GDPR requires regulated parties to employ "privacy by design," which it

[7] https://www.bloomberg.com/graphics/2016-amazon-same-day/

defines as using "technical and organizational measures" to protect individual "rights and freedoms." As described above, successful implementation of privacy by design will require privacy and IT governance professionals to work closely together to develop management systems and controls that bake in privacy throughout the organization. The GDPR also codifies a "right of erasure" (a codification and expansion of the "right to be forgotten") which allows an individual to request erasure of his or her personal data where the "data are no longer necessary in relation to the purposes for which they were collected or otherwise processed."[8] Exceptions exist for processing that is necessary to freedom of expression, to the public interest in the area of public health, and to other specified purposes. This right thus requires organizations to take a set of legal criteria and apply them to particular facts to reach a conclusion about whether to grant the removal request. The IT governance professionals who will guide their organizations with respect to the "right of erasure" will need to become more familiar with this type of legal analysis, an area in which their privacy counterparts have much experience. The GDPR punishes non-compliance with penalties of up to four percent of a company's worldwide turnover. This makes the GDPR's privacy requirements a true corporate governance concern that merits the attention of IT governance professionals, and not just a matter of privacy compliance. Organizations whose IT governance and privacy professionals work closely with one another will best be able to thrive under this new and significant regulation.

Federal Trade Commission policies are creating a similar imperative. Increasingly, FTC consent decrees require alleged violators to institute comprehensive privacy management programs and submit to third-party audits. Privacy professionals

[8] General Data Protection Regulation, Art. 17, https://gdpr-info.eu/art-17-gdpr/

who draw on the expertise of their IT governance colleagues and gain a solid understanding of the organization's existing management systems, administrative controls and audit mechanisms will be much better prepared to negotiate and implement these agreements. By the same token, IT governance professionals who are familiar with the privacy field will best be able to ensure that the new, comprehensive privacy programs are consistent with, and leverage, other internal management and audit systems.

Conclusion

Businesses and other organizations understand well the benefits that come from breaking down internal walls and working in cross-functional teams. Viewed from this vantage point, the continuing divisions between the cybersecurity, privacy and IT governance fields constitute something of an anachronism. The expansion of the data-driven economy, and of the laws that govern it, requires lowering these walls. The organizations that perceive this and encourage their data governance professionals to gain fluency in each other's areas — to become cyberpros — will be best prepared to manage the new challenges successfully.