Building a Privacy Culture

Privacy is the right to be free from interference or intrusion. Information privacy is most often associated with digitization, but information privacy has been an issue ever since personal information started to be stored on and processed by mainframe and mini-computers. Since that time, work performed by privacy professionals has led to the enactment of a number of privacy laws and regulations around the world.[1] Fair information practices identify how an information-based society should access and store information while maintaining privacy.[2]

Personally identifiable information (PII) is any data that can be used to identify a specific individual. Social Security numbers, postal or email addresses, and telephone numbers are commonly considered PII. Other PII includes Internet Protocol (IP) addresses; log-in identifiers; social media posts; digital images; and geolocation, biometric and behavioral data.[3]

Because of emerging technologies, protecting information privacy has become more challenging. Unfortunately, there is no easy solution to this situation. Corporate culture reflects the priorities, objectives and assumptions of management and staff. Changing corporate culture to ensure a focus on information privacy can be a prolonged and painstaking process that requires strategic support and direction from senior management. In today's data-driven economies, boards of directors (BoDs) and c-level management are responsible for the strategic direction and shape of the corporate privacy program.

Information Privacy

Whereas information security is focused on protecting information from unauthorized access, information privacy ensures that any information an enterprise receives, stores, processes and shares is handled based on the wishes of its customers and users. In short, security protects data, and privacy protects identity.[4] Data masking techniques can protect privacy by hiding PII while data are stored, processed or presented to users, whereas encryption ensures security by protecting information from unauthorized disclosure. Industry-specific regulations have been designed to mandate how enterprises deal with PII throughout its life cycle.

Data privacy (also called information privacy or data protection) is about the collection of, access to and use of data, and the data subject's legal right to those data. Data subjects are entitled to expect the following:

- No unauthorized access to private data
- No inappropriate use of data
- Accurate and complete collection of personal data by technology
- Access to and ownership of data content
- The right to inspect, update or correct data[5]

Privacy Culture

Enterprises are living entities, and their culture helps them survive in today's fiercely competitive business environment. Senior management and

Muhammad Asif Qureshi, CISA, CIA, CISSP, PMP
Is a governance, risk management and compliance (GRC) professional with an extensive background in information systems auditing. He is currently a GRC manager with the Tawazun Economic Council, where he was involved in establishing its information security department and building its information security architecture.

Enjoying this article?

- Read *A Global Look at Privacy 2020: Trends in Privacy Practices. www.isaca.org/global-privacy-2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

BoDs share the responsibility for implementing a corporate culture that is in line with corporate strategy, legal and regulatory requirements, and business ethics. Technology-driven enterprises must integrate systems, products and electronic information affecting individuals into the privacy culture. Privacy-compliant business processes, systems and products impact business practices, which develop into privacy norms (**figure 1**).

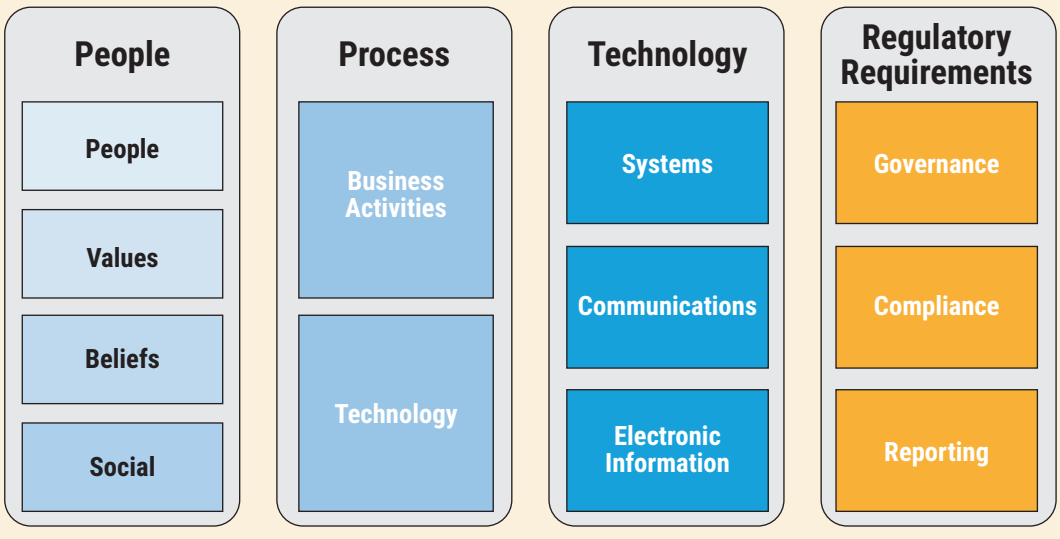
The diversified nature of a privacy culture and the need for its integration throughout an enterprise can make it difficult to implement and maintain. Emerging technologies can disrupt existing business practices related to data integration, consolidation and communication. Information is multifaceted and does not reside on a single server. Systems that access this information are impacted by the regulatory requirements to protect PII. As a result, enterprises are finding it necessary to develop cultures, processes, practices and systems for maintaining the privacy of PII. Because enterprises operate in a highly regulated environment, the roots of privacy culture can be found in the laws and regulations developed to protect PII. These laws address the rights and obligations of both customers and organizations.

Regulatory Landscape

Modern-day cyberthreats have increased the need to protect businesses' reputations and gain customers' confidence. Legislative bodies and other entities have responded by developing regulations to control the processing and transfer of PII. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) published ISO/IEC 27701, the first international standard for the management of information privacy. Several countries and groups of countries have developed their own privacy laws to ensure the data privacy of their citizens and residents:

- **Asia Pacific Economic Cooperation (APEC)**—In 2005, APEC developed a privacy framework for its 21 member countries. It comprises nine privacy principles: preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability. The APEC Privacy Framework promotes a flexible approach to information privacy protection, while avoiding unnecessary barriers to the flow of information. The framework provides guidance and advice to enterprises operating in APEC countries by

Figure 1—Components of a Privacy Culture



highlighting common privacy matters, the impact of privacy issues on organizations and consumer expectations, with the goal of helping enterprises conduct business in a way that is consistent with the principles outlined in the framework.[6]

- **European Union**—In 2018, the EU General Data Protection Regulation (GDPR) replaced the Data Protection Directive. The GDPR mandates the protection of PII of residents and citizens of the European Union irrespective of their physical location—that is, both inside and outside the European Union. The rules do not apply to data processed by an individual for purely personal reasons or for activities carried out in an individual's home, provided there is no connection to a professional or commercial activity. When an individual uses personal data outside the personal sphere, such as for sociocultural or financial activities, the GDPR must be respected.[7]
- **United Kingdom**—The United Kingdom passed its own version of the GDPR, known as the UK-GDPR. It will run parallel with the EU's GDPR until the end of the Brexit transition period, which is expected to end on 31 December 2020. During the transition, all EU laws will continue to apply in the UK, after which the GDPR will become a UK law. Enterprises based in both the UK and the EU will need to update their privacy notices to reflect the change in status. The UK government plans to continue enforcing the GDPR, so enterprises should maintain compliance.[8]
- **Canada**—Canada regulates the protection of personal information held by enterprises through the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). The former relates to individuals' right to access and correct personal information held by federal government institutions, whereas the latter sets the rules for the collection, use and disclosure of personal information by private-sector enterprises. PIPEDA does not apply to enterprises that are not engaged in commercial, for-profit activities, such as charities and political parties. Alberta, British Columbia and Quebec have their own private-sector laws. Enterprises in the Northwest Territories, Yukon and Nunavut are covered by PIPEDA.[9]

> "DATA PRIVACY IS SERIOUS BUSINESS, AND THIS IS REFLECTED BY THE PENALTIES AND FINES IMPOSED ON NONCOMPLIANT ENTERPRISES."

- **Australia**—In Australia, data privacy is regulated through a mix of federal and provincial laws. The Federal Privacy Act was introduced to protect the privacy of individuals and to regulate how government agencies and enterprises with an annual turnover of more than US$1.9 million handle personal information. Except for Western Australia and South Australia, most states and territories have their own data protection laws. The Federal Privacy Act includes the following principles: Individuals have the right to be anonymous, and enterprises must clearly express their privacy policies, collect only requested information, inform individuals about data collection, ensure the protection of information before overseas disclosure, and take steps to protect personal information from misuse, unauthorized access, modification and disclosure.[10]
- **United States**—The United States has several sector-specific and information-specific national privacy and data security laws, including laws and regulations that apply to financial institutions, telecommunications organizations, personal health information, credit report information, children's information, telemarketing and direct marketing.[11] The US Federal Trade Commission (FTC) has broad authority to enforce laws that protect data privacy. Most regulations that protect data privacy are at the state level. They include the US State of California Consumer Privacy Act (CCPA) and the New York Consumer Privacy Act (NYCPA); Massachusetts and Minnesota also have data privacy laws. The growing number of state-level laws will provide a baseline for the development of a comprehensive federal data privacy law.[12]

In January 2020, the US National Institute of Standards and Technology (NIST) issued its Information Privacy Framework,[13] which follows the

structure of its Cybersecurity Framework (CSF).[14] The NIST framework is a set of voluntary procedures that can help enterprises across the globe with different data protection requirements. It provides a structured approach to data privacy in countries with fragmented data privacy laws.

Data privacy is serious business, and this is reflected by the penalties and fines imposed on noncompliant enterprises. Some data breaches and the resulting fines have captured media attention:

- Facebook was fined US$5 billion, which is, by far, the largest penalty ever imposed for violating customers' privacy rights.
- British Airways was hit with a penalty of US$230 million.
- Marriott was fined US$124 million.
- Equifax agreed to pay a minimum of US$575 million for its 2017 breach.
- Uber's 2016 breach cost it almost US$150 million.
- In April 2018, the US Securities and Exchange Commission (SEC) fined Yahoo US$35 million for failing to disclose a breach that affected its entire database, or about 3 billion accounts.[15]
- Tesco Bank was hit with a £16.4 million (US$21.2 million) fine in 2018 by the UK's Financial Conduct Authority (FCA) for a 2016 breach that resulted in just under US$3 million being stolen from 9,000 customer accounts.[16]
- In 2017, retail giant Target agreed to a US$18.5 million settlement with 47 US states and the District of Columbia related to a 2013 breach in which some 40 million credit and debit card accounts were stolen.[17]

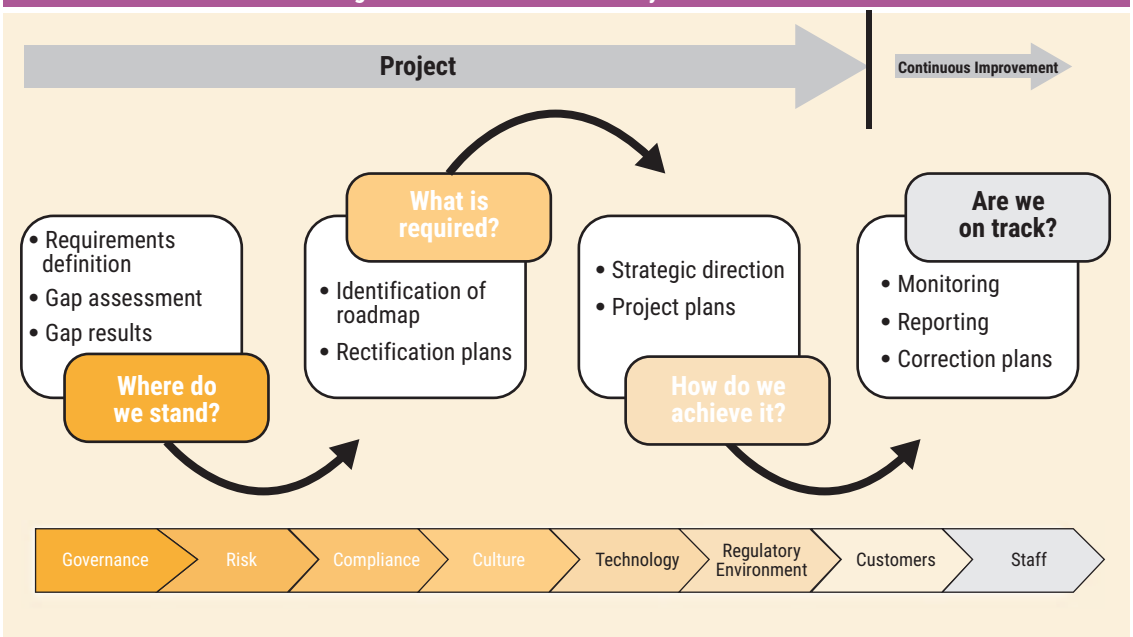
Creating a Privacy Culture

In an effective privacy culture, protecting PII is of paramount importance. The privacy culture should closely align with an enterprise's value system. It is vital to implement strategies to convert privacy knowledge into repetitive practices to shape culture over time.[18]

To establish a privacy culture, follow these steps outlined in **figure 2**:

1. **Identify and understand the current state of privacy**—Consider performing a gap assessment. Refer to the requirements of applicable privacy laws to arrive at an assessment model. This step is challenging, as it involves translating legal

Figure 2—How to Create a Privacy Culture



requirements into implementation requirements, but it should be done with care because the results will lead to corrective actions. Missing any key privacy requirements can jeopardize the whole exercise and skew the resulting decisions. It is critical to perform a privacy risk assessment relevant to business processes. Consider the technology and systems in use and how privacy risk may impact the scalability of these systems. Depending on the complexity of business operations, this step can take a few weeks to a few months.

2. **Identify areas that need improvement**—Once the results of the initial assessment are received, areas in need of improvement should be apparent. These areas might range from the enterprise's governance model to day-to-day operations. The next step is to develop rectification plans. It is best to start with the governance level, as management commitment is crucial to building a privacy culture. Without senior management's support, strategic initiatives will not bear the desired results. Establish a connection between privacy requirements and the enterprise's business objectives, and obtain executive management's sign-off. It is imperative to show the value of a privacy culture by improving the enterprise's brand value and reputation and avoiding potential fines and legal difficulties.
3. **Develop a privacy policy and relevant governance components**—Executive management should be able to envisage the benefits of a privacy policy. Consequently, a project needs to be initiated to integrate the privacy policy into business processes (see **figure 3**). The resources needed to complete this project should be estimated and the necessary approvals obtained. Return on investment (ROI) can be questioned by senior management, and this should be matched with the avoidance of fines, improved brand image and impact on business value. The gaps identified in step 1 should be referred to, and implementation plans should be developed in coordination with process owners. Engage the project management office (PMO) to manage the project, and include senior management as project owners and sponsors.
4. **Track and monitor progress**—Report the project's progress to stakeholders, and obtain their endorsement and continuous support.
5. **Establish a program for ongoing monitoring and improvement**—Once the initial assessment project is completed, develop a roadmap in the shape of a privacy program with key performance indicators (KPIs) for periodic monitoring and continuous improvement.

Information Privacy Scorecard

Keeping c-level management informed of privacy activities within the enterprise is essential to ensure their continuous support. One way to do this is to compile and distribute an information privacy scorecard (**figure 4**). Scorecards not only depict current performance but also identify areas of improvement for senior management attention.

Figure 3—Integration of Business Processes and Privacy Policy

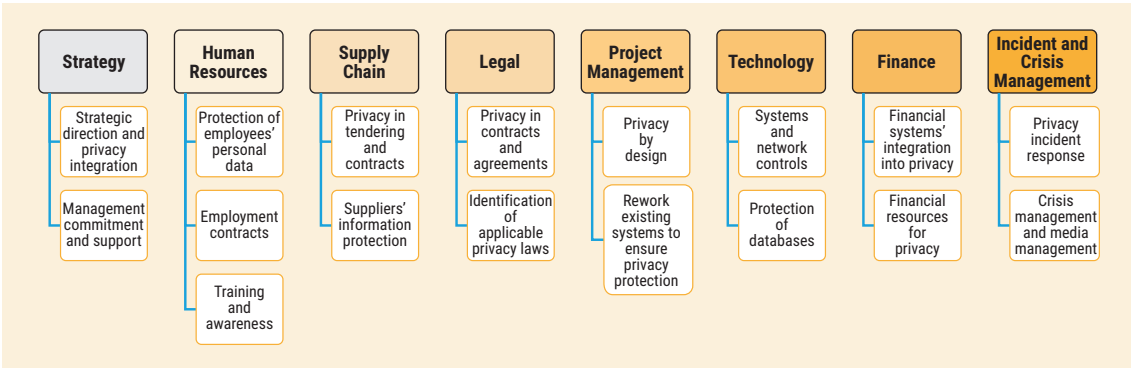
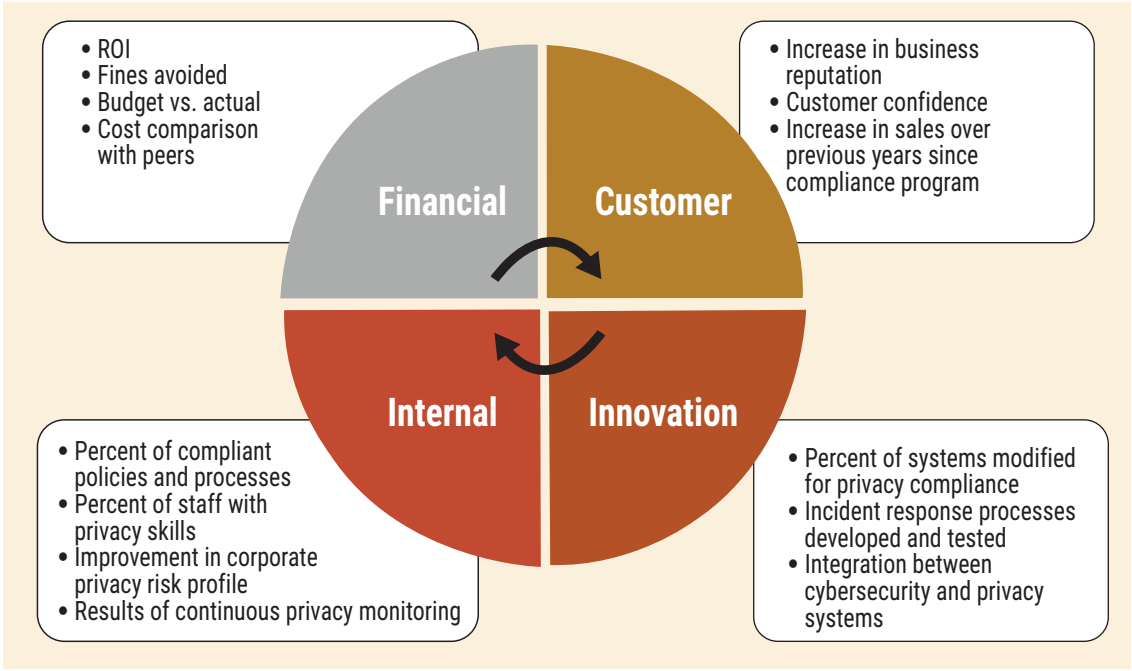


Figure 4—Information Privacy Scorecard



As a matter of fact, revenue generation, cost minimization and return on investment as a result of privacy culture core areas of interest for senior management. Revenue targets can be achieved when customers are satisfied with the enterprise. As a response to customer's expectations for data privacy, the enterprise should improve its internal processes and operations, which can result in enhanced internal capacity and efficiency through innovation and learning. This can be examined from four perspectives : financial, customer, innovation and internal.

When developing a scorecard, privacy professionals should consider the data sources and the integrity of the information produced by these sources. Information privacy is changing the way enterprises do business, so data should be obtained from all business functions. Sometimes scorecards also contain information obtained from third parties, in which case the authenticity of the information and the independence of the third party should be considered.

Financial

Financial aspects of data privacy include calculating ROI on data privacy investments. To put it in numbers, references can be made to the customer confidence index as a result of data privacy measures. Customer confidence may be represented by an increase in usage of e-commerce sites or an increase in the number of online transactions or number of mobile app downloads. Financial benefits can be identified by looking at the improvement in processes that resulted in avoiding fines. Budget vs. actual cost is most known for financial measures. Comparing the cost of the deployment of a data privacy program with industry peers can identify the effectiveness of deploying financial resources.

Customer

An increase in positive feedback from customers and stakeholders is an indicator of business reputation and value. In financial terms, business reputation can be looked at in terms of credit rating, share price, business goodwill, etc. Customers will feel more comfortable when they trust that their information is going into safe hands. Data privacy disclosures on the organization's website and other electronic media will boost customer confidence. As a result, the organization may experience an upward trend in sales and revenue numbers as a result of a matured data privacy program.

Innovation
As more and more organizations are IT-driven, the systems supporting business processes should be in line with data privacy policies. A measure of success for data privacy can be the number of IT systems modified to be in compliance with privacy policies. On a different note, organizations should be prepared to deal with data breaches. The level of preparedness of an organization for dealing with a data breach is a strong indicator of a successful data privacy program. An integral part of a data privacy program is to have an inventory of data held by the organization and implement security controls based on the profile of data. This needs a seamless integration between data privacy and cybersecurity tools. A KPI can be set on the level of integration between these tools.

Internal
Internal audit reports can be very useful when identifying the number of policies complying with legal and regulatory requirements. Trainings and workshops attended by the staff are a good indicator of increasing data privacy knowledge among staff. Corporate risk profiles improve as a result of controls implemented during the execution of a data privacy program. This shows how effectively organizations are managing their risk. Similarly, continuous monitoring results in timely identification of gaps and rectification plans, which improves overall efficiency and effectiveness.

Addressing the Challenges

Implementing a privacy culture can be a challenging task if it is not managed properly. Changing an enterprise's culture is never easy, and every enterprise faces unique challenges. However, that should not deter efforts to create a privacy culture that is in line with global best practices, meets stakeholders' expectations and navigates the murky waters of compliance requirements. Some of these challenges include the following:

- **Technology**—With the advent of new technologies and their complex architecture, data privacy has become even more of a challenge. Internet of Things (IoT) devices collect personal information that is stored in the cloud. Similarly, artificial intelligence (AI) and machine learning integrate with systems and import information for analysis through algorithms that are often beyond the understanding of most individuals. Data Privacy professionals should be engaged to analyze information collected by these technologies and the controls deployed for protecting this information. Privacy while data are at rest and in motion should be considered.

"WITH THE ADVENT OF NEW TECHNOLOGIES AND THEIR COMPLEX ARCHITECTURE, DATA PRIVACY HAS BECOME EVEN MORE OF A CHALLENGE."

- **Changing legal landscape**—The enactment of myriad privacy laws presents a challenge, especially for enterprises with a global presence. Interpreting multiple privacy laws and regulations can be overwhelming, and privacy professionals are continually struggling to keep up-to-date with new and revised privacy laws, determine their applicability and ensure that the enterprise is in compliance. Organizations should consider developing integrated legal frameworks that align with business strategy and operations.
- **Third parties**—Outsourcing business activities is a common practice. The situation becomes even more complicated when business is outsourced to an enterprise in a different geographic location with an entirely different legal landscape with regard to privacy. This can make ensuring that third parties are complying with relevant privacy laws a difficult task. Contractual obligations for compliance with local privacy laws should be considered. Management should also consider conducting independent compliance reviews on a periodic basis.
- **Lack of resources**—Complying with privacy laws often requires both financial and human resources. These resources may not be available due to conflicting business priorities. Privacy professionals must identify risk factors and potential consequences if adequate resources are not allocated. Data privacy professionals should have access to C-suite management to ensure that these risk areas are adequately addressed.

- **Lack of management commitment**—Management may be focused on maximizing profits and reducing costs. As a result, compliance with privacy regulations may be far down on management's list of priorities. Seasoned privacy professionals understand the risk of ignoring privacy compliance issues and must bring this to the attention of the right level of management.
- **Cultural resistance**—Cultural change must be adequately planned and enforced, while keeping in mind the existing culture and values of the enterprise. Privacy professionals should be sensitive to the feelings of staff impacted by cultural change. Sharing information and knowledge with staff can help gain their support and commitment. Sufficient training should also be part of the campaign.

> "PRIVACY PROFESSIONALS MUST IDENTIFY RISK FACTORS AND POTENTIAL CONSEQUENCES IF ADEQUATE RESOURCES ARE NOT ALLOCATED."

Auditing Information Privacy

The objective of a privacy audit is to ascertain that the enterprise's privacy posture is in compliance with applicable privacy laws and industry best practices. The audit typically includes an assessment of processes throughout the information life cycle. Internal auditors are best suited to provide such assurance, but skillful and knowledgeable third parties can also perform these audits. The benefits of privacy audits include improved compliance with regulations, policies and practices and enhanced awareness among management and staff.

Global auditing bodies, including ISACA® and the Institute of Internal Auditors (IIA),[19, 20, 21] have issued guidelines for conducting privacy audits. Internal audits can evaluate the privacy framework, identify significant risk factors, make appropriate recommendations to enhance the privacy framework and identify applicable privacy laws.

Conclusion

In today's data-driven world, information is the lifeblood of many organizations. While the focus is on generating revenues and sustaining operational efficiency, it is equally important to ensure that an information privacy culture and process exist. Enterprise reputation and customer confidence, which act as catalysts for revenue generation, are sustained through a robust privacy culture.

Implementing a privacy culture is a considerably longer journey that demands perseverance. Success in this endeavor needs thorough planning and support from senior leadership.

Protecting information privacy need not be seen as a compliance burden; it can be an added value to the enterprise if it is implemented in the right spirit. Enterprises must engage all stakeholders and strike the right balance between managing the risk and reward of information privacy.

Endnotes

1 Mulligan, D. K.; C. Koopman; N. Doty; "Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy," *Philosophical Transactions of the Royal Society A*, 28 December 2016, *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5124066/*

2 Dixo, P.; "A Brief Introduction to Fair Information Practices," January 2008, World Privacy Forum, *https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/*

3 Grimes, R. A.; "What Is Personally Identifiable Information (PII)? How to Protect It Under GDPR," *CSO Online*, 22 August 2019, *https://www.csoonline.com/article/3215864/how-to-protect-personally-identifiable-information-pii-under-gdpr.html*

4 Phillips, D.; "Data Privacy vs. Security: What Is the Core Difference?" Tokenex, 1 August 2019, *https://www.tokenex.com/blog/data-privacy-vs-security*

5 Lee, W. W.; W. Zankl; H. Chang; "An Ethical Approach to Data Privacy Protection," *ISACA® Journal*, vol. 6, 2016, *https://www.isaca.org/archives*

6 CTI Sub-Fora and Industry Dialogues Groups, Digital Economy Steering Group (DESG), "APEC Privacy Framework," Asia-Pacific Economic Cooperation (APEC), 2005, *http://apec.org/Publications/2005/12/APEC-Privacy-Framework*

7 European Commission, "What Does the General Data Protection Regulation (GDPR) Govern?" *https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en*

8 National Law Review, "Post-Brexit Data Protection: Where Are We Now?" 4 February 2020, *https://www.natlawreview.com/article/post-brexit-data-protection-where-are-we-now*

9 Office of Privacy Commissioner Canada, "Summary of Privacy Laws in Canada," *https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/*

10 DLA Piper, Data Protection Laws of the World, Australia, *https://www.dlapiperdataprotection.com/index.html?t=law&c=AU*

11 DLA Piper, Data Protection Laws of the World, United States, *https://www.dlapiperdataprotection.com/index.html?t=law&c=US*

12 Brooks, R.; "U.S. Privacy Laws: State-Level Approaches to Privacy Protection," Netwrix Blog, 27 August 2019, *https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/*

13 National Institute of Standards and Technology (NIST), "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management," USA, 16 January 2020, *https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf*

14 National Institute of Standards and Technology (NIST), Cybersecurity Framework, USA, 2013, *https://www.nist.gov/cyberframework*

15 US Securities and Exchange Commission, "Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million," 24 April 2018, *https://www.sec.gov/news/press-release/2018-71*

16 Higgins, B.; "Message for Current Account Customers," 2016, *https://yourcommunity.tescobank.com/t5/News/Message-for-Current-Account-customers/td-p/6599*

17 Swinhoe, D.; "The Biggest Data Breach Fines, Penalties and Settlements So Far," *CSO Online*, 31 January 2020, *https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html*

18 Bustin, K.; "Practical Strategies for Creating a Privacy Culture in Your Organization," International Association of Privacy Professionals (IAPP), 24 August 2018, *https://iapp.org/news/a/2010-08-24-strategies-for-creating-a-privacy-culture-in-your-organization/*

19 Interniaudit, "Managing and Auditing Privacy Risks," *https://www.interniaudit.cz/download/ippf/GTAG/gtag_5_managing_and_auditing_privacy_risks.pdf*

20 Institute of Internal Auditors (IIA), "Auditing Privacy Risks," *https://na.theiia.org/standards-guidance/Member%20Documents/PG%20Auditing%20Privacy%20Risks.pdf*

21 ISACA®, *Data Privacy Audit Program*, 2017, USA, *https://www.isaca.org/bookstore/audit-control-and-security-essentials/wapdp1*