COSMOS
Navigate the Compliance Universe

CEP Magazine - January 2020
Budgeting considerations for continuous monitoring of data privacy and security

By Ambler T. Jackson, CIPT, CIPM, CIPP US/G, JD

Ambler T. Jackson (amblertjackson@gmail.com) is a privacy subject matter expert located in Washington, DC, USA.

- linkedin.com/in/amblertjackson/

Businesses traditionally continuously monitor performance. In the digital age that we live in—and considering the amounts of personal data collected, used, and shared by businesses, organizations, and governments—monitoring performance is no longer enough. Businesses and organizations must also monitor data-driven business practices (e.g., collecting and sharing personal data) and information technology (IT) systems that process personal data. Cyberattacks involving the compromise or loss of personal data are becoming increasingly more common for organizations and businesses that collect, maintain, and use personal data. Compromised personal data may lead to identity theft of the data subject, embarrassment, or reputational harm to the compromised company. Therefore, continuous monitoring of business practices and IT systems is not only the appropriate, and in some cases mandated, course of action—it is simply the right thing to do.

Today, many organizations have a cybersecurity program. Depending on the size and the industry, a privacy program may fall within the organization's larger cybersecurity program. Perhaps both privacy and security fall under the broader cybersecurity program. Some organizations may only have a privacy program, and no cybersecurity program at all. Others may simply have an IT department that focuses on security, but considers data privacy when necessary to meet a business need. Regardless of how data privacy and security is embedded in the organization, it will be necessary to continuously monitor activities that may pose a risk to data privacy and securing data assets. Continuously monitoring business practices and IT systems that collect personal information is required to appropriately manage risk. Implementing such a program requires resources, and a budget is required to obtain those resources.

Budgets for continuous monitoring activities will vary. The budget for a Big Tech company and the United States government will not be the same. Similarly, the budget for a new start-up in the online retail space and a new healthcare service will not be the same. In September 2018, the White House released the National Cyber Strategy, which reinforces ongoing work and provides strategic direction for the federal government to act on short- and long-term improvements to cybersecurity for the government, private sector, and individuals. The National Cyber Strategy: (1) recognizes that private and public entities have struggled to secure their systems as adversaries have increased the frequency and sophistication of their malicious cyberactivities, and (2) directs the federal government to do its part to ensure a secure cyber environment for our country. The FY 2020 President's Budget includes $17.4 billion of budget authority for cybersecurity-related activities, a $790 million (5%) increase above the FY 2019 estimate.[1]

Challenges to requests for a budget

Requesting budget approval for continuous monitoring activities may be new for many organizations, and a

how-to reference does not exist. Traditionally, organizations did not have a budget line item for cybersecurity or privacy programs. With the emphasis placed on the importance of data privacy and security in both the private and public sector, the risk management discussions related to budgeting for activities that will mitigate risks associated with collecting, processing, and securing personal data are increasing. Although there appears to be greater importance placed on data privacy as of late, there are still many challenges related to obtaining approval for a budget that supports continuous monitoring activities. Smaller companies often do not have the budget to engage in adequate continuous monitoring activities. Depending on their data practices and industry, leadership may not see the value in having a budget for continuous monitoring activities. Larger organizations may not include a budget line item for the programs that require continuous monitoring because they are currently paralyzed with the arduous task of identifying all of their data assets, systems, and associated risks. An organization cannot continuously monitor what they do not know about.

Additionally, challenges include the fact that, initially, it may be difficult to place a dollar amount on managing risks from a data privacy and security perspective. Depending on the size of the organization and the types of data involved, it may be labor intensive and costly to fully identify and understand the business practices and IT systems that involve personal data and the associated risks. Finally, there is no one-size-fits-all budget for these activities, and every organization will need to take a tailored approach to creating their continuous monitoring budget. Consider that Joe's online bicycle shop in Florida will not be able to use the budget that Sally's online retail shop in the European Union uses. The two shops will have different continuous monitoring needs based on their data collection practices, business processes, and location.