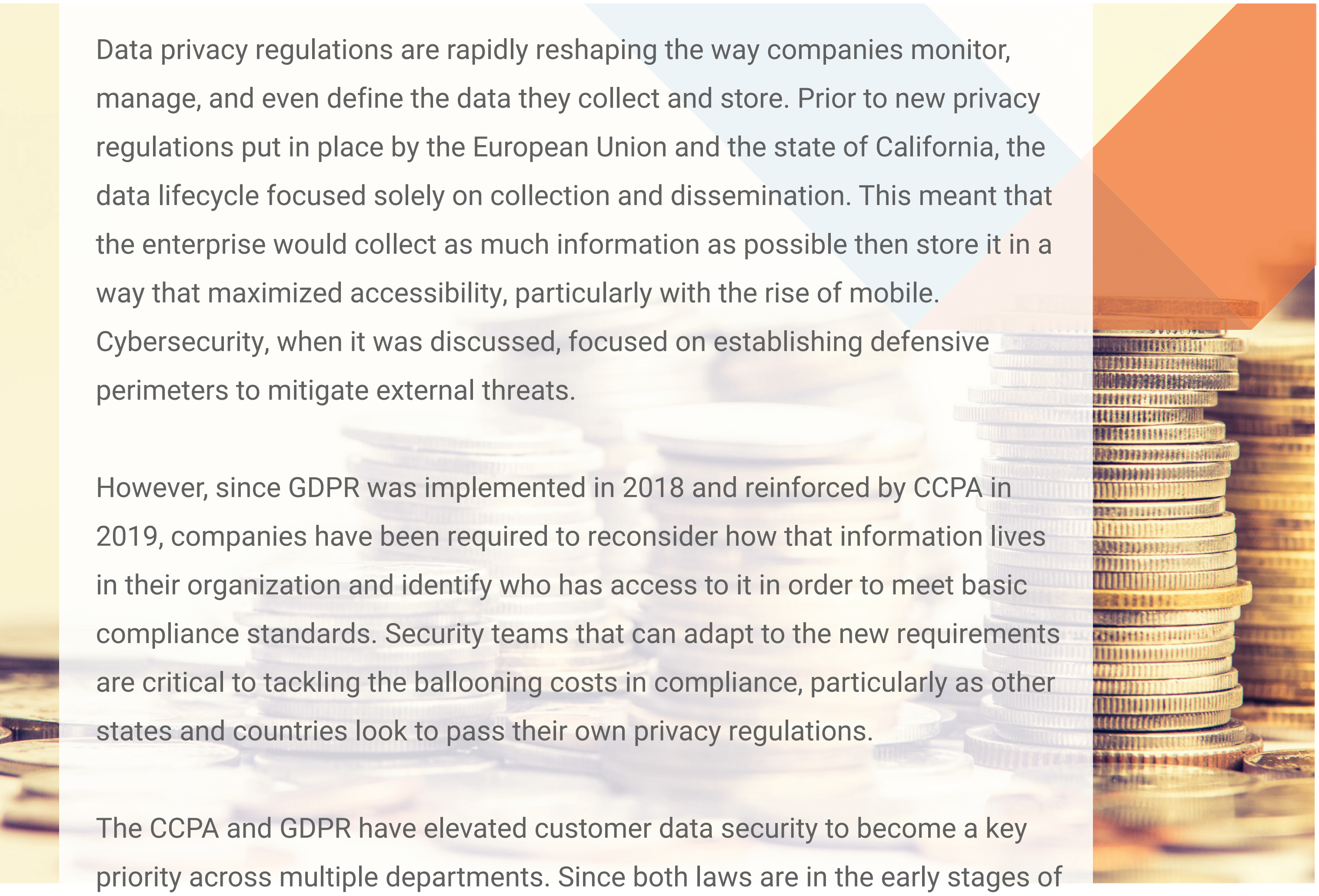
APPSIAN

EXECUTIVE BRIEF

Managing Compliance Costs with Enhanced Cybersecurity Visibility

Greg Wendt | Executive Director - Security



Data privacy regulations are rapidly reshaping the way companies monitor, manage, and even define the data they collect and store. Prior to new privacy regulations put in place by the European Union and the state of California, the data lifecycle focused solely on collection and dissemination. This meant that the enterprise would collect as much information as possible then store it in a way that maximized accessibility, particularly with the rise of mobile. Cybersecurity, when it was discussed, focused on establishing defensive perimeters to mitigate external threats.

However, since GDPR was implemented in 2018 and reinforced by CCPA in 2019, companies have been required to reconsider how that information lives in their organization and identify who has access to it in order to meet basic compliance standards. Security teams that can adapt to the new requirements are critical to tackling the ballooning costs in compliance, particularly as other states and countries look to pass their own privacy regulations.

The CCPA and GDPR have elevated customer data security to become a key priority across multiple departments. Since both laws are in the early stages of implementation and interpretation by enforcement agencies, legal departments have become an essential ally in compliance. In the case of the GDPR, the right to be forgotten has been contested by search giant Google in several high-profile court cases, adding greater nuance and detail to how the law impacts data management. Human resources is also a valuable partner in compliance management as they are best positioned to engage employees on new security protocols and assist in the successful deployment of new technology to ensure that workflow is not disrupted.

Legacy infrastructure increases compliance costs

The CCPA alone is expected to cost enterprises $55 billion in initial compliance costs, with additional costs to be expected in maintenance fees, with IBM's 2019 Cost of a Data Breach Report states that the average total cost of a data breach increased to an average of $3.92 million in 2019, though in the United States the average cost per breach rose to $8.9 million. Much of that cost is driven by the recovery process, which involves understanding how the system was breached, what information was affected and bringing systems back online. For many organizations, understanding the scope of damage is difficult because current security systems aren't designed for data visibility or access management, both of which enable security teams to track who has accessed what data and when.

Data visibility is a particularly acute challenge in ERP systems because they contain highly sensitive business data, such as financial information, intellectual property or insurance details. Since ERP systems hold so much valuable data, they're often the last piece of the digital infrastructure to be updated. This results in security gaps when patches are missed, or new security features are added to a legacy system. The "black box" of ERP systems can cause delays in damage assessments, resulting in the risk of hefty fines as the GDPR requires affected customers to be notified within 30 days of when information is compromised.

Organizations lack tools to comply with “right to know”

Compliance costs have largely been driven by the wave of “right to know” and “right to be forgotten” requests from their users. The right to know establishes the right of the consumer to know exactly what data a company has collected on them, and to download that data. For the enterprise, this requires being able to identify, organize and share all information pertaining to every single user, breaking the black box paradigm that existed before GDPR. Recent research shows that each request is estimated to cost approximately $1,400, quickly adding to compliance costs.

The right to be forgotten allows consumers to request that any data related to them be deleted from an organizations’ database. Though the rule is less broadly applicable than the right to know, organizations should be careful of potential violations in their third-party partners or even of careless practices by employees.

For GDPR and CCPA compliance, outdated and disparate infrastructure also adds major challenges, especially when adhering to the response time limits set out by GDPR. The law requires that organizations respond to right to know requests within 30 days. Yet a global survey of 103 companies worldwide across various industries found that 58% of respondents were unable to meet data access and portability requests within the one-month time limit. One of the main barriers to timely right to know requests was the lack of consolidated, transparent data structures that made finding all relevant information on each individual a costly and long process.

When organizations don’t understand where collected data is or who can access it, compiling a right to know report is next to impossible. Without any means of tracking access within their internal databases, most enterprises have no idea if the personal information of any user has been accessed, copied or stored in multiple places, forcing compliance teams to track down each piece individually and risking fines when request response takes longer than 30 days. Not only does this heighten the likelihood of compliance violations, but also contributes to the rise of insider security threats, particularly in highly sensitive fields like healthcare and finance.

As a result, security and compliance teams have begun joining forces to better understand the lifecycle of business data in the enterprise and how it can be effectively secured.

Regulations align with industry trends

In many ways, the new regulatory pressures brought by the CCPA and GDPR align with emerging trends in cybersecurity. Insider threats are one of the fastest growing trends in data breaches, accounting for 34% of attacks in 2019. Security features that enable granular tracking of user behavior in real-time addresses ensures access management can be done accurately while also adhering to privacy standards set forth by the GDPR and CCPA. As a result, organizations improve both security and compliance because they can be better prepared to respond to insider threats, minimize direct damage caused by a breach as well as void penalties incurred by compromising customer data. With greater means to identify and differentiate users, security teams are also able to increase access controls as well as better understand who has modified data and when.

The GDPR and CCPA have had a significant impact on the public expectation for privacy and security. While security measures like multi-factor authentication (MFA) and complex passwords have existed for years, consumers and developers frequently opposed requiring them due to concerns over adding too much friction to the user experience. With cybersecurity concerns entering the mainstream, many consumers are actively seeking out additional ways to protect and manage their personal data. For the enterprise, this has increased employee's receptiveness to new security features such as MFA to internal systems. Particularly with complex ERP systems, system administrators can unify the heightened expectations for security created by the GDPR and CCPA to reduce the costs of compliance.

Advanced security tools can address challenges experienced across all departments by supporting secure migrations, enabling better data visibility in new systems, and reducing the long-term costs of compliance. As the security discussion evolves to when not if a hack takes place it is essential to have a holistic program in place to understand what actions will be taken when data is compromised. By hiding their head in the sand, the unprepared enterprise not only risks more damaging attacks but also larger fines. The right security tools can lay the foundation for a program that effectively fulfills the multidisciplinary role of security and engages all necessary experts to protect data and minimize compliance costs.

This article was originally published by CPO Magazine.

Written by

Greg Wendt, Executive Director - Security at Appsian is a Oracle® PeopleSoft security expert. During his 17 year career, he has been recognized as a leader in data security, application architecture and business operations. He served as ERP Application Architect at TCU where he was responsible for TCU's PeopleSoft system and was Chairman of the Higher Education User Group's multinational Technical Advisory Group (HEUG TAG). Greg has led criminal justice and cyber security courses focusing on hacking techniques.

APPSIAN

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

☎ +1 (469) 906-2100

✉ info@appsian.com

www.appsian.com