4 Reasons ERP Data Security and Privacy Should Factor into Your 2021 Security Budget

Piyush Pandey • CEO, Appsian

The COVID-19 crisis uncovered many data security and privacy gaps that organizations have spent the better part of 2020 trying to fill — largely exposed by the quick and drastic shift to remote workforces. Now many organizations are considering how 2021 objectives will impact their current cybersecurity budget.

As organizations look to strengthen their enterprise data security and privacy programs, they must consider the new risks that remote work has uncovered. More specifically, how legacy business applications and ERP systems may be exposing organizations to new levels of risk because these applications were not designed for user access from unmanaged networks and devices.

ERP Data Privacy and Data Governance Must be Top Priorities

2020 has seen a parallel emphasis on cybersecurity, data privacy, and data governance. On top of hackers looking to exploit applications and steal data, remote workforces have brought data privacy and data governance into the spotlight. An organization's ability to continue with normal business operations in a remote environment without seeing a significant increase in fraud and data exploitation has been an overlooked challenge of 2020. One that has forced many leaders to quickly establish privacy and compliance frameworks.

As it relates to business data, organizations must establish strict policies to support data privacy and governance, as well as establish the technical controls required to enforce those policies. The latter being a significant challenge for organizations using legacy business applications with remote workforces. With risk being defined mainly by the context of a user's access, dynamically enforcing governance is a crucial objective that requires additional investment.

An investment in solutions like GRC, data masking, attribute-based access controls, stepped-up authentication, and visibility into data access & usage all support an organization's objective to minimize risk, enable data security and data privacy.

Go Beyond a VPN With Defense in Depth

When organizations rapidly shifted to remote workforces, many rushed to purchase virtual private networks (VPNs) to help protect data. VPNs act as a data "tunnel" by creating a secure connection with another network over the internet, usually using encryption to reduce the impact of a cyberattack. However, VPNs do not protect data once a user is authenticated – especially if authentication results from a compromised credential from a phishing attack. Once a user's credentials are authenticated, risks like data exfiltration, overexposure of data, and fraud committed inside financial transactions remain significant challenges for organizations to manage.

Although VPNs provide value, assuming a VPN enables data security is a common misconception. Without taking the context of access into account, the risk remains high. For example, where is a user coming from? What data are they trying to access? What device are they using? Is that device being used by the right person?

Without a doubt, VPNs provide an essential service. However, as organizations continue remote work, they need to put additional protections around sensitive data - not just the ability to authenticate into applications. As part of your 2021 budget plans, you need to consider investing in solutions that help you bolster your VPN services with a layered data security strategy that goes beyond authentication.

Dynamic Workforces Require Dynamic Authorization Strategies

Most organizations recognize the value of authentication as a primary identity control. However, authentication alone only addresses half of an organization's security requirements. While authentication seeks to validate that the user is who they say they are, user authorization establishes policies that govern specific access privileges. In short, ERP data security and governance hinge on user authorization just as much as user authentication. If not more.

Implementing authorization strategies that are dynamic and risk-aware becomes critical when access is coming from unmanaged networks and devices. This is because the risk derived from a user's access is based mainly on the context of that access.

For example, high privilege activity taking place overseas, during non-work hours, or on personal devices all present high levels of risk – solely because of the context of what that user is doing and how they are doing it.

Legacy ERP applications, especially on-premise applications, lack the ability to authorize user privilege dynamically, leading to a user being over-privileged based on what they are currently trying to do. To mitigate this risk, organizations should invest in attribute-based access controls and having the ability to dynamically manage access based on various contextual situations specific to a user.

Invest in Advanced Analytics to Gain Visibility into User Behavior

Detecting anomalous activity or behavior indicative of risk is especially challenging because separating the bad from the good (or the authorized) requires granular visibility. This is especially challenging when moving your workforce out of the office and away from managed networks and devices.

Companies lose approximately 7% of their annual revenue to fraud. In a year that will likely have slim revenue margins, 7% of revenue is a larger number than before. With a remote workforce, visibility into user behavior becomes more critical than ever, as workers no longer have people around them who might see fraudulent actions.

Tracking user behavior within mission-critical ERP solutions enables organizations to detect potentially fraudulent behavior faster. Internal fraud poses a different problem than credential theft. With credential theft, detecting outlier access with contextual controls can mitigate the risk (for example, Blacklisting IPs from hostile countries). However, internal malicious actors use their legitimate access during their regular working hours. Moreover, with employees working from home, they might have more opportunities to misuse their access.

Ultimately, organizations need to invest in solutions that provide real-time data analytics that captures access usage and establishes the appropriate audit trails to use if they need to engage in forensic analysis.

Investing in a Remote Workforce Means Investing in ERP Data Privacy and Governance

From a business standpoint, COVID-19's impact will endure long beyond the development and dissemination of a successful vaccine. According to IBM's "COVID-19 and the Future of Business" report, 64% of respondents shifted to more cloud-based business activities, and 55% made permanent changes to organizational strategy. Additionally, a survey conducted by Twilio noted that COVID-19 accelerated companies' digital transformation strategy by an average of six years. Combining these statistics, 2020's business story is that companies took only 10 months to accelerate their operations strategies that were originally scoped to take 6 years.

Ultimately, the bulk of an organization's 2021 budget should continue to enable modernization strategies. Especially those that seek to evolve and secure the core business applications that are so influential on business operations and long-term strategic goals.

Piyush Pandey, CEO at Appsian Security is a technology executive with 18 years of global experience in strategy, sales, mergers & acquisitions, and operations within software companies. Over the last 10 years, Pandey has advised companies on the software space and on enterprise performance and security, working with leading technology companies such as Oracle, Epicor, Concur, Citrix and Microsoft on various transactions.

APPSIAN SECURITY

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

☎ +1 (469) 906-2100

✉ info@appsian.com

www.appsian.com