World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:17, No:01, 2023

Addressing Supply Chain Data Risk with Data Security Assurance

Authors : Anna Fowler

Abstract : When considering assets that may need protection, the mind begins to contemplate homes, cars, and investment funds. In most cases, the protection of those assets can be covered through security systems and insurance. Data is not the first thought that comes to mind that would need protection, even though data is at the core of most supply chain operations. It includes trade secrets, management of personal identifiable information (PII), and consumer data that can be used to enhance the overall experience. Data is considered a critical element of success for supply chains and should be one of the most critical areas to protect. In the supply chain industry, there are two major misconceptions about protecting data: (i) We do not manage or store confidential/personally identifiable information (PII). (ii) Reliance on Third-Party vendor security. These misconceptions can significantly derail organizational efforts to adequately protect data across environments. These statistics can be exciting yet overwhelming at the same time. The first misconception, "We do not manage or store confidential/personally identifiable information (PII)" is dangerous as it implies the organization does not have proper data literacy. Enterprise employees will zero in on the aspect of PII while neglecting trade secret theft and the complete breakdown of information sharing. To circumvent the first bullet point, the second bullet point forges an ideology that "Reliance on Third-Party vendor security" will absolve the company from security risk. Instead, third-party risk has grown over the last two years and is one of the major causes of data security breaches. It is important to understand that a holistic approach should be considered when protecting data which should not involve purchasing a Data Loss Prevention (DLP) tool. A tool is not a solution. To protect supply chain data, start by providing data literacy training to all employees and negotiating the security component of contracts with vendors to highlight data literacy training for individuals/teams that may access company data. It is also important to understand the origin of the data and its movement to include risk identification. Ensure processes effectively incorporate data security principles. Evaluate and select DLP solutions to address specific concerns/use cases in conjunction with data visibility. These approaches are part of a broader solutions framework called Data Security Assurance (DSA). The DSA Framework looks at all of the processes across the supply chain, including their corresponding architecture and workflows, employee data literacy, governance and controls, integration between third and fourth-party vendors, DLP as a solution concept, and policies related to data residency. Within cloud environments, this framework is crucial for the supply chain industry to avoid regulatory implications and third/fourth party risk.

Keywords : security by design, data security architecture, cybersecurity framework, data security assurance
Conference Title : ICCACS 2023 : International Conference on Computer Architectures and Computer Systems
Conference Location : New York, United States
Conference Dates : January 30-31, 2023