7 Ways to Address the Gaping Data Security Hole in Your Supply Chain

Computerworld pointed out recently a fast growing trend: the emergence of CDOs, or Chief Data Officers. The CDO role is the authority on all things data management and data governance. Computerworld defines it as follows: the mission of the chief data officer is to bring order to the plethora of data sources within an organization, tap the multiple analytics opportunities that exist, and develop a strategic vision around those opportunities.

The challenge has been that different departments store their own data independently, with their own policies and tools, including practices for data distribution. With the rise of big data investments, combined with a string of high profile data breaches at some of the biggest company names in the world, data is front and center. Data security is a top priority within the enterprise. Rightfully so. But a major area of business remains overlooked and un-addressed when it comes to data security: the supply chain.

For most companies, the tens or hundreds of trading partners scattered throughout the globe that produce and move their ingredients, parts, materials and finished goods from production to the end customer, are a gaping risk. Most supply chains are global. Crossing multiple countries. Involving anywhere from 5 to 25 parties in a single transaction. And every time an order, amendment or information signal of any kind moves from one supply chain partner to another, the risk of a breach or data interception grows. While businesses are deploying CDOs to maintain a handle on data within the enterprise, the movement of data in the supply chain is very much the old Wild West — with spreadsheets and emails frequently being fired across the globe.

We hear about personal information being stolen all of the time. But what about corporate information and the impact on the brand? Picture a pharmaceutical company shipping drugs or a firearms company shipping ammunition. Container loads of goods are moving across the globe. It’s critical that nobody knows what’s in those containers or has data to locate them. If the wrong person gets their hands on supply chain data, they can highjack or steal the ammunition or drugs. This can be as easy as intercepting an email or EDI signal. This poses a huge risk to retailers and manufacturers.

The Supply Chain Data Challenge

Supply chains are series of separate businesses. No matter how secure an enterprise is within its four walls, once data is sent outside, those security measures are worthless. Transmitting data all over the world and placing it into the hands of trading partners equates to a loss of data control. Every time data moves outside the organization, the threat grows greater. Conversely, the less data moves around, the more secure it can be. Easier said than done. But here are seven traits to look for in a supply chain collaboration strategy to improve data security.
1. Move the data as little as possible. Rather than sending data all around the world, have external partners come to the data. How? Connecting all parties on a single cloud platform is the starting point. The key is to house all of the supply chain data at the core of the network, where all supply chain parties can see it, act on it and collaborate on it. A single instance database plugged into a multitenant network allows external parties to come to the data — eliminating insecure emails, Excel spreadsheets and EDI.

2. When data does move — and it has to — deploy secure protocols such as AS2. Strong encryption is needed anytime data is in movement.

3. Take a close look at how data is stored on the platform. Make sure the data system and legal structure are secure. Ask about and confirm the control layers around employees of any service provider handling your data.

4. A cloud supply chain platform should have a security policy that you can review. Ask for security control details when speaking to a vendor. This should illustrate security controls applied, such as authentication.

5. Your cloud supply chain vendor should have external security penetration testing done constantly. This should include hiring ethical hacking services to infiltrate the site. They should be able to provide status of security at all times. In addition, internal process audits, such as SSAE 16, should be standard policy.

6. Service providers should have a documented and audited change management process in place. Any change to service or code should happen through that document system. It should include details around sign offs.

7. Request to see a vendor’s DR and business continuity plan. They should be able to document drills and processes. If a meteorite hits the data center, for example, the service provider should be able to demonstrate the ability to recover. But what if the service provider’s offices are inaccessible? This is where business continuity is important.

Keeping customers’ information safe is very important. But don’t let that blind you to the gaping hole in your supply chain. Connect with your trading partners. Find a way to bring them all into a single online ecosystem, where they can come to the data, instead of sending the data to them. This is the first step in addressing the data security risk in every global supply chain.

---

Keys to Look Out for to Ensure Data Safety

Privacy: messages have to be encrypted. All data and traffic between users is stored and protected in the cloud centrally.

Integrity: data stored by a provider has to be assured integrity. This means only the appropriate person can change it. It’s necessary to have access to a history of every change. This is done with digital signatures. A private key pair can be used to electronically sign all documents. This allows the end user to know that nobody has made any data changes over time.

Legal framework — non-repudiation: similar to a contractual physical signature, non-repudiation makes documents legal. It means the signature came from that person. Nobody can challenge it.