In the world of cyber, your supply chain is in danger

Re-engineering your logistics communications can safeguard your organization's lifeblood

By Karen Puchalsky

When companies think about re-engineering their supply chain, they think about modernizing or improving their manufacturing process.

And if your company does not manufacture a product, you may not even think of yourself as part of the supply chain. But in reality, whether you manufacture a product or offer a service, you are part of the supply chain, as illustrated in Figure 1.

Unless your company has migrated to a new enterprise resource planning application like Oracle or SAP, it is likely that the applications that support your supply chain have been untouched for years. If this is the case and the applications have not been re-engineered, your company is undoubtedly vulnerable to harmful cyberattacks, and you are spending more money to maintain your outdated supply chain. After all, old processes can be inefficient and can expose your company's critical and sensitive data to attacks.

Many supply chains utilize a form of electronically generated data that is sent to customers, suppliers and other third-party providers. One example, Electronic Data Interchange (EDI), has been around for more than 30 years. Because of its longevity, once a company implements it, updates and other major changes are rarely made, making the electronic documents of EDI the "forgotten environment" shown in Figure 2.

FIGURE 1

Where do you fit?

No matter your business – manufacturing or service – your company is part of a supply chain.

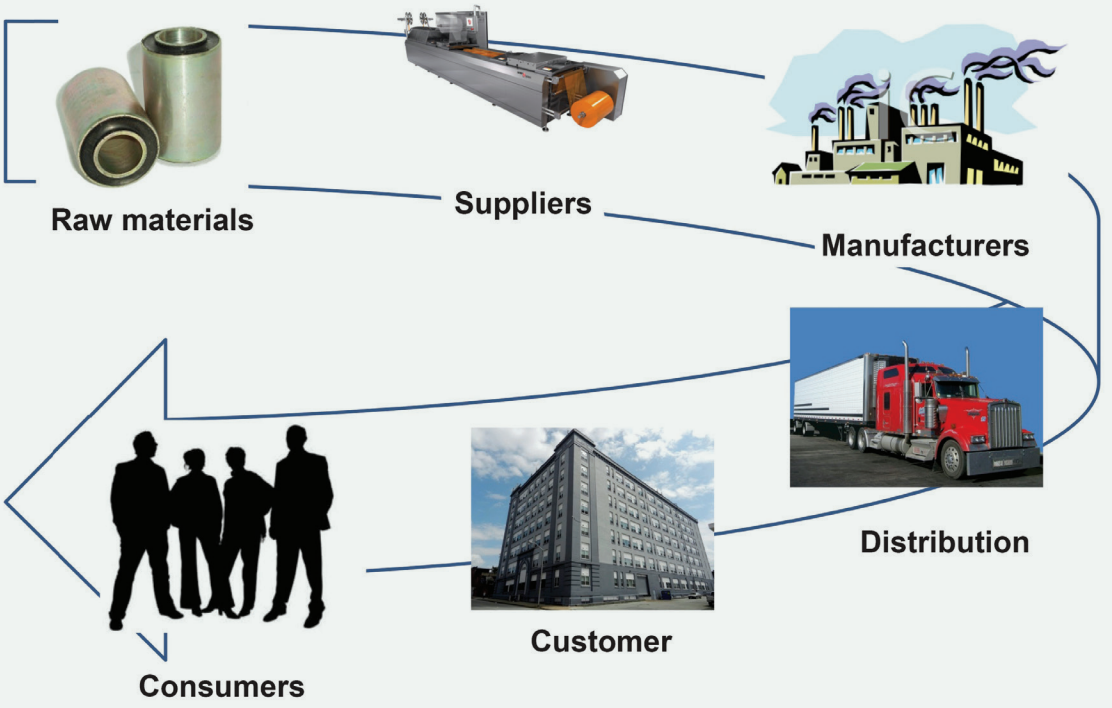
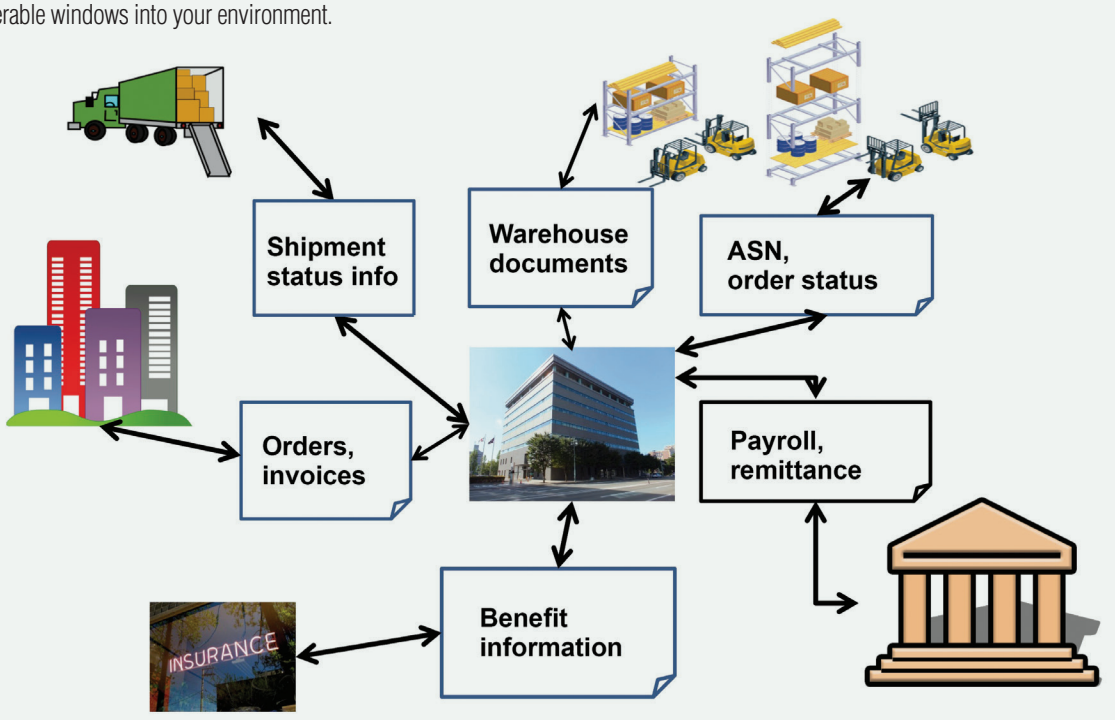


FIGURE 2

Open windows are dangerous

Many electronic documents are sent and received to support the supply chain. Communicating to all these partners opens potentially vulnerable windows into your environment.



The supply chain is a company's lifeblood; it is the complete order to cash process that keeps every company in motion. So why aren't companies protecting their lifeblood? It's stable, but is it secure? Where do you start to ensure your company is running efficiently and safely?

When re-engineering their supply chain, companies often make the big mistake of immediately starting to implement the new environment without understanding the current one. If you don't understand the old environment, trading partner requirements and the flow of data, your operations team can make a lot of mistakes in the re-engineering process, adding time and cost to the project.

It is imperative that you begin by evaluating several areas within your supply chain process:

- Classification of your data
- Backups and recovery processes
- Connectivity to your business partners

Classification of your data

Before you start to re-engineer your supply chain, you need to classify the data that the process supports. Start by asking the following questions:

- Does the data have to meet any compliances, such as HIPAA, PCI-DSS or others?
- What data, if acquired by your competitors, could be detrimental to your company?
- Who has access to your data?
- How is the data edited, changed and shared?

Evaluating and classifying your data is important to ensure you re-engineer your processes so you stay in compliance while securing your data from malicious or accidental breaches. How the data is shared is key to ensuring that critical or sensitive data is not shared either accidently or maliciously. One company evaluated its data and found that employees were sharing HIPAA information through emails, which could violate regulatory and security protocols. How are your employees sharing your data?

Backups and recovery processes

These parts of your processes usually get the least amount of attention, budget and testing – even though without proper backup and recovery processes, you may not recover from a major outage. This can result in an enormous financial risk, loss of credibility and decline in customer confidence.

If you are breached and need to restore your entire supply chain environment, how long until you can be back online? How long can you survive without access to your critical data? How long can you support your customers without access to your data? And what happens to the lost data?

It's important to assess your backup procedures to make sure you can get back online as fast as possible with minimum impact to your company and your customers. For example, if you receive orders continuously throughout the day and you only back up this process once a day, what happens to all the orders received between the backups? How is it recovered, or is it lost forever?

Connecting to your business partners within your supply chain

Improving your firewall, antivirus software and web portals are often the first things that come to mind when assessing how to protect your company's data against cyberattacks. You probably are not looking internally at your supply chain, and you may not realize that the amount of business partners you are trading with can represent the number of "windows" that are open in your environment.

Look at how you are connecting to your business partners first. What type of protocols are you using? Many companies are still using file transfer protocol (FTP) to connect to their business partners. Recently, the FBI became aware of criminal actors who are actively targeting FTP servers to access critical information operating in "anonymous" mode. Research conducted by the University of Michigan in 2015 titled, "FTP: The Forgotten Cloud" indicated that more than 1 million FTP servers were configured to all anonymous access, potentially exposing sensitive data stored on the servers. Cyberattackers also use the anonymous mode to store malicious tools that can be launched at a later time. Some malicious tools can sit up to 200 days before they are activated.

Other protocols can be used that are more secure, but there should be someone at your company who monitors these "windows," ensuring they have not been compromised. If you don't have someone on site, you should consider a secure communications provider to manage all the connectivity to your supply chain partners.

Most companies have logs of all their communications. But the questions should be: "Who is responsible for monitoring these logs? How do they know that a breach has occurred? And perhaps even more importantly, what are the processes and procedures followed when a breach has happened?"

The supply chain is your company's lifeblood. Protecting the supply chain from cyberattacks is imperative to ensure your company operates smoothly and efficiently. If you haven't looked at your processes since EDI was implemented three decades ago, maybe it's time. ❖

Karen Puchalsky is founder, president and CEO of Innovate E-Commerce, which provides business-to-business managed services. Puchalsky and her company have earned numerous awards, including the INC 500 award, Pennsylvania's Best 50 Women in Business and the Top 25 Women in Business by the Pittsburgh Business Times.