In recent times, large corporations are increasingly concerned about damage to their brand reputation resulting from high-profile cyber-attacks. Organizations struggle to protect their confidentiality, integrity, and availability of data. With new innovations in technology such as storage of big data, cloud-based solutions, and predictive analysis, information security has also become more complex. These matters are further complicated with electronic solutions like automatic procure-to-pay systems and e-sourcing. Furthermore, humans are another weak link in the supply chain. These include manufacturers, importers, transporters, agents, and third-party logistics providers. Cybercriminals who aim to attack organizations mainly for ransom, can attack any of these vulnerable layers.

# The Key Cybersecurity Risks

Cyber-attacks are not always straight forward. Most businesses depend upon service providers and third-party suppliers to carry out operations. Many of these trusted relationships are important suppliers of products or services such as IT, accounting, or marketing. Any weak link in the supply chain can be a security threat for an organization.   
  
Let’s have a brief look at some major cybersecurity risks in the supply chain management:

## Third Party Suppliers

Your organization may have cyber-security policy in place but what about your suppliers that need to access your system to perform routine business? Often, it’s the smaller companies that have contract with larger companies that are targeted due to being more vulnerable. A small company that only provides a good or service can have vital information while having little or no security implementation.

The problem that comes next is the suppliers of your suppliers, also called second tier suppliers. As an organization, you may have addressed all security vulnerabilities in your software but your solution provider may still have a security weakness. Poor practices of security by second tier suppliers can completely bring a company down.

A cyber-attack can result in breach of intellectual property, critical data breach custody, interrupted operations, and a decrease in service level provided to the end user.

## Software Solution Providers

Your organization can also suffer a cyber attack through a counterfeit software or hardware with embedded malware delivered to you. To reduce infrastructure costs, supply chain functions are usually outsourced to solution providers. Most of these data aggregators and website builders are at a risk of malware attacks where attackers find vulnerability in a website and attack it.

## Lack of Employee Awareness

Humans are the weakest link in an organization’s security. Even with all security mechanisms in place, a careless move from an employee can cause losses to an organization. This is why training and education of employees is recommended, along with the key suppliers. Moreover, Bring Your Own Device (BYOD) policies in the supply chain can result in security breaches. Usually, the level of malware detection and protection in mobile devices is not adequate. Furthermore, with more phishing scams getting successful every passing day, it is important to focus on training human resources about how to be vigilant and how to respond in uncertain situations.

## Risks Associated with Smart Products

Technologies like IoT and [smart](http://www.cardzgroup.com/ContactLessSmartCard.html) devices are helping immensely in managing supply chains, but they also come with big risks. By combining physical and digital components, digitizing supply chain has opened up the attack surface.

Additionally, with the proliferation of smart products with sensors and embedded codes, cybersecurity risks in the supply chain have increased.

# The Road Forward – How to Mitigate Risks in Supply Chain

Apart from brand damage and financial loss, a cyber attack can also lead to critical data and intellectual property breach. To improve cybersecurity in the supply chain, it is important to improve the quality of relationship among all the members involved.   
Here are a few ways to ensure safety:

* Create a first-respondent team in times of cyber crisis. This team should plan for contingency and perform risk management while re-arranging the resources.
* Improve and secure the processes, such as due diligence of new suppliers and strong guidelines for supplier access to your assets.
* Train employees as well as suppliers directly or indirectly involved in the process about security procedures and best practices.
* Use smart devices that come with regular patches and updates.

It is important for companies to invest in supply chain capabilities that can identify and withstand cyber-attacks to ensure a safe and secure supply chain management process.