NEW CYBERSECURITY REQUIREMENTS for Supply Chains
The last few years have demonstrated the threat of cybercriminals on the world’s supply chains. In the wake of COVID-19, malicious hackers have increasingly exploited vulnerabilities in networks and applications across supply chains. The US alone saw supply chain attacks rise by 42% in just the first quarter of 2021—impacting over seven million people.\(^i\)

In the face of this renewed global threat, countries have taken decisive (and sometimes radical) steps to tackle the problem head-on.\(^{ii\,iii\,iv}\)

### Recent Developments in Global Cybersecurity

**US:** The government’s Cybersecurity Executive Order to tackle new digital threats.

**UK:** Recent amendments to the Product Security and Telecommunications Infrastructure bill to secure 5G rollout against cyberthreats.

**Thailand:** The Personal Data Protection Act (PDPA), effective from 2020, to increase regulation against any external company that processes or stores personal data of citizens.

These worldwide cybersecurity attacks and subsequent measures to address them may have been a prominent wake-up call for industries. But this is just the first step in a complex path to create robust supply chains amid a slew of digital dangers.
Safeguarding our Supply Chains in a Hostile World

Criminal organizations have used weaknesses in supply chains to get critical data, which has caused immense damage to supply chains worldwide. The JBS and Colonial Pipeline incidents are just two of the most recent examples of such attacks. The JBS incident had deep ramifications, as the attack shut down its operations for a short time in Canada, Australia, and the US. The entirety of the damage was attributed to the presence of compromised passwords that allowed criminals to infiltrate the supply chain. The Colonial Pipeline hack was a ransomware attack that inhibited the flow of around 100 million gallons of refined fuel that the pipeline moved every day. This accounts for about 45% of all fuel used on East Coast of the United States.

The volatile environment after COVID-19 gave cybercriminals more opportunities to take advantage of vulnerabilities in the systems, resulting in fallouts. With ever-present and complex threats, a change was crucial in securing cyber resilience.

The complex ecosystem of contributors that make up today’s supply chains is reliant on collaboration and transparency. In this landscape, third-party contractors and vendors are a core part of supply chain operations, with their access to the hiring company’s internal systems. This presents unique risks, because while a company can always outsource its functions, it can never pass on the responsibility to safeguard its data to these contractors. A 2019 survey has highlighted that, out of 600 reviewed businesses, approximately 44% experienced a data breach caused by third-party vendors.

Data is getting all the love and protection from industries forming fortresses of cybersecurity, but supply chains are still at risk from many weak points. Touch points ranging from manufacturers and partners to service providers and suppliers are the most vulnerable. It is no wonder we are witnessing such current dire straits, with regards to cyber health.
Challenges Across Verticals
What Supply Chain Security Means for Each Industry

From manufacturing to retail, each industry is evolving towards a more digital landscape with more complexities. Unique attack vectors and industry-specific challenges provide unique opportunities for cybercriminals to work their way into supply chain systems. ix

Manufacturing

The risks associated with unmanaged access to end points have been a major concern in ensuring cybersecurity across industries. For the manufacturing sector, many new techniques and tactics utilized by cybercriminals has ravaged the industry. Per a 2020 report x, this sector is one of the most targeted industries via malicious browser breaches, comprising over 38.6% of all global attacks. x

Phishing-based attacks have also been a huge risk for the manufacturing sector. With a lack of security awareness the threat doubles in scope. Monitoring these threats across shadow IT devices and all end points has been a great challenge for the industry.

Energy and Natural Resources

A completely new threat landscape exists today due to the immense pressure to integrate with the dominant digital revolution. Assistive tools and approaches in remote operations have oftentimes become weak points exploited by cybercriminals. This is why one of thee industry's top risk areas includes IT/OT integrations and malware. Remote integration operations in the current landscape have opened up new avenues for cyber criminals to compromise entire networks that were previously harder to access. This is why incidents like the Colonial Pipeline breach have taken place— wherein hackers exploited weaknesses in the existing IT integrated systems.xi

The attack has also led to a number of US governmental initiatives to regulate and boost cybersecurity. The most prominent of these was the cybersecurity executive order that called for federal governments and private sector enterprises to work together for modernizing the country’s cybersecurity.xii
Key Initiatives of the US Cybersecurity Executive Order:

- A standardized playbook and set definitions for federal responses to cyber incidents
- Improved data sharing within the federal government via an endpoint detection and response system
- The removal of contractual barriers that might stop IT service providers from flagging cybersecurity breaches
- The presence of a “Cybersecurity Safety Review Board”, comprising public and private sector members, which can analyze situations and suggest further recommendations
- IT service providers reporting to the government about dangerous cybersecurity breaches
- A push for the federal government to upgrade to secure cloud services and deploy other mandatory cybersecurity measures (such as multifactor authentication, encryption etc.) within a specific time frame
- Improved security for software sold to the government, including the public sharing of certain security data by developers

Pharmaceuticals

Alongside shadow IT, a major cause for concern has been with maintaining endpoint cybersecurity. Industry leaders have shown concern about preventing risks from third-party consultants and contractors. In fact, pharmaceutical supply chains face ransomware susceptibility that tops almost $31 million dollars annually. xiii

Such hyperextended and high-risk supply chains necessitate several layers of security to ward off cybercriminals. This has given rise to logistical issues, with more exchange points creating several end points primed for cyber-manipulation. The biggest challenge for an industry as critical as pharmaceuticals is perhaps maintaining cybersecurity best practices across end points and third-party contractors.
Addressing the Security Question
A Holistic Initiative

The first step towards a more resilient supply chain is gaining complete visibility. This is achieved when stakeholders from multiple departments come together with similar goals in mind. It’s not enough for the IT team to mandate certain protocols; procurement, health and safety, operations and other departments must understand the reasoning behind the rules, and how to best implement them.

The Three Pillars – People, Process, and Technology

Begin by analyzing the three areas where cyber security risks occur—people, processes, and technology. Keen visibility on these vulnerable areas and quick responses to mitigate breaches should be implemented decisively.
Government-Corporate Collaboration

As local governments begin to implement cybersecurity regulations, companies will see improvements in their operations. Some of these benefits include:

- Greater transparency between governments and businesses
- Developing standardized requirements through collaboration
- More secure software design and supply chains, including a greater emphasis on easy-to-secure digital technologies (cloud, multi-factor authentication, incident tracking, SaaS, etc.)

Through this co-working framework, we expect to see more returns from security investments. Furthermore, this will open up the door for international collaboration and cooperation, where best practices can be shared and insights tabulated for more globally cohesive supply chain cybersecurity.

Third-Party Risk Assessment and Management

Businesses must be able to categorize their contractors when determining access to enterprise data. Risk assessment and regular audits ensure that organizations can trust their third-party vendors to maintain their cybersecurity obligations.

Assessing and creating a “cyber risk profile” for all third-party partners is the first crucial step, with a few important considerations to keep in mind:

- The type of data that can be shared
- How that data can be shared safely
- The level of access that each third-party vendor will have
- Impact of disruption on third-party production schedules

With these parameters in place, companies can begin management as required. This includes assigning specific service-level agreements (SLAs) for each contractor that will allow them to regulate cybersecurity standards across the entire supply chain ecosystem. Alongside this, limited network access and regular reviews of supply chain end-points ensure weaknesses are quickly rectified. Finally, clear guidelines on data ownership and acceptable use must be established for contractors as well.
The Avetta Outcome

Avetta provides a cybersecurity assessment prequalification form to all its clients so that they gain visibility into how their suppliers are exposing them to potential risks in several areas. These include data privacy, electronic communications, web presence, IT sourcing, and even payment processing. This visibility mitigates one of the bigger risks clients face: auditing suppliers for security. Oftentimes, effort is spent ensuring third-party suppliers are trustworthy. The transparency provided by a partner, such as Avetta, provides much-needed stability and security to clients in a singular platform.

Avetta understands that every supply chain presents its own unique features and risk cases. In this ecosystem, a holistic framework is essential to maintain security and business continuity: something that Avetta One provides on one platform. As the industry’s largest supply chain risk management (SCRM) platform, Avetta One is a singular, end-to-end supply chain risk mitigation solution. With Avetta One, organizations enjoy the following benefits:

- A supplier risk assessment that evaluates vendor adherence to critical security controls like the use of communications protocols, data management, and IT system management.
- Easy scheduling of cyber assessments at customized intervals and flagging of cyber risks to trigger notifications and risk workflows.
- A proactive approach towards cybersecurity by provisioning cybersecurity audits through trusted partners.
- Assessments of suppliers’ digital security and risk management practices to identify the cyber resilience of vendors.
- The ability to ensure proper training for suppliers to use sensitive information and protect it with appropriate tools.

The need for resilient supply chains will remain for as long as they keep evolving. However, with the help of SCRM platforms like Avetta One, both clients and suppliers can manage supply chain risk and become more qualified to conduct operations respectively. Avetta One is a one-stop shop that monitors supplier safety, sustainability, workforce competency, and overall performance. Through comprehensive contractor prequalification across major industries, the platform ensures the safety and security of enterprises’ supply lines in an evolving cyber-threat landscape.
About Avetta

The Avetta SaaS platform helps clients manage supply chain risk, and their suppliers, to become more qualified for jobs. For the hiring clients in our network, we offer the world’s largest supply chain risk management network to manage supplier safety, sustainability, worker competency and performance. We perform contractor prequalification and worker competency management across major industries, all over the globe, including construction, energy, facilities, high tech, manufacturing, mining, and telecom.

For suppliers in our network, our audit and verification services help lower their safety incidents rate by 29%. As a result, about 50% of members find additional job opportunities within the first year of joining. In addition, our suppliers receive privileged access to the Avetta Marketplace, where dozens of partners offer special discounts for business services like insurance and work gear. Avetta serves more than 500 enterprise companies and over 125,000 suppliers across 120+ countries.