Loss Control Considerations for the Transportation of **Server Racks and Supercomputers**

The transportation of server racks and supercomputers presents several material risks that should be carefully managed. These assets are high in value, physically sensitive, and are often shipped under time-sensitive conditions. While typically free of data during transit, they remain critical components in data centre and enterprise infrastructure projects. This article outlines the principal risks associated with road and air transport and provides guidance on appropriate control measures.

Server Racks and Supercomputers

Server racks are modular frameworks used to house standardised IT hardware such as servers, switches, and power distribution units. They are a common feature in data centres and are often shipped either empty or preloaded with components. Supercomputers, by contrast, are highly specialised high-performance computing systems designed for complex processing tasks. While they may be physically housed within rack-like enclosures, supercomputers are typically bespoke, consisting of densely integrated hardware and requiring more specialised handling due to their sensitivity and configuration complexity.

Server racks and supercomputers vary in size, weight, and configuration. Some are shipped fully assembled with internal components such as blades, power supplies and cooling systems; others are transported as empty enclosures. The risk profile is significantly higher when internal hardware is present due to the increased sensitivity to mechanical shock and environmental conditions. Despite the absence of data on board, the high cost of equipment and the operational importance of timely installation can make loss events potentially severe.

Risks in Road Transport

Road transport accounts for most damage incidents. Mechanical shock and vibration during transit are key concerns, particularly when road surfaces are poor or vehicles lack appropriate suspension systems. Unsecured or poorly balanced cargo can shift in transit, leading to tipping or collapse. Manual handling during loading and unloading introduces further risk, especially if forklifts or lifts are not correctly aligned with rack dimensions or crate construction.

Theft is another exposure, particularly when equipment is clearly marked or identifiable. Layovers at unsecured facilities and inadequately trained personnel can increase the likelihood of opportunistic theft or mishandling. Environmental conditions during loading, unloading or storage may also affect sensitive components. Exposure to high humidity, dust, or temperature extremes can compromise electronic parts, particularly where packaging does not offer sufficient protection.

Risks in Air Transport

Air transport offers faster transit times and reduced exposure duration but introduces its own set of risks. Ground handling at airports is a frequent cause of damage. Crates may be dropped, tilted, or stacked incorrectly. Despite standard labelling, fragile cargo is often subject to rough handling in high-volume environments. This risk is elevated during transshipments or customs inspections.

Another concern is environmental exposure on the tarmac. In hot or humid climates, equipment may be exposed to temperature fluctuations and moisture during loading delays or while awaiting clearance. If not properly wrapped, there is also the potential for wet damage, whilst waiting. While aircraft holds are typically pressurised and temperature-controlled, conditions during ground handling can be less predictable. Coordination between freight forwarders, handlers and airline staff is critical to maintaining handling standards across all stages.

Risks in Sea Transport

While air and road are the most common modes for high-value electronics, marine transport is sometimes used for international movements where cost sensitivity outweighs time constraints, however, it is discouraged for high value shipments.

One of the primary marine transport concerns is prolonged exposure to vibration and mechanical stress. Ocean voyages can last several weeks, during which equipment is subjected to continuous low-frequency movement caused by vessel motion. This can result in cumulative stress on components, especially where internal hardware is installed or packaging lacks appropriate cushioning.

When shipped in sealed containers, equipment is vulnerable to condensation due to temperature fluctuations between day and night or when passing through different climate zones. Moisture ingress can cause corrosion or degrade sensitive electronics and insulation materials. This is particularly problematic for shipments that are not fully vacuum-sealed or controlled. The risk is increased in older containers or those not fitted with desiccants.

Containers holding sensitive IT equipment may be stacked below deck or adjacent to cargo that produces heat or emits corrosive vapours. Poor segregation during loading can compromise the shipment’s integrity. Crates or racks not properly braced within containers may shift or fall if subjected to rough seas, terminal handling, or crane operations during transshipment.

Loss Control Recommendations

- Shipping components in separate packages or crates, rather than as fully built servers or supercomputers can significantly reduce the risk of damage during transportation.
- Crates should be purpose-built to the specifications of the equipment, with adequate internal bracing, cushioning, and structural reinforcement.
- Packaging should be tested to ensure it can handle the expected dynamic forces of the conveyance method. There have been incidents where the racking system has collapsed, causing considerable damage.
- Shock and tilt indicators should also be considered. Depending on the value of the shipment, live tracking, with parameters defined by the Original Equipment Manufacturers (OEM).
- The use of anti-vibration pallets should be used, if considered necessary.
- Handling instructions should be clearly displayed on all visible surfaces in accordance with internationally recognised packaging symbols.
- Equipment should be secured inside crates to prevent movement and should not bear weight from stacking.

- Crates should be tightly wrapped with stretch film or shrink wrap covering the whole crate.
- Hauliers and forwarders should have documented experience with high-value electronics.
- Vehicles used for road transport should be equipped with air-ride suspension.
- Drivers should be trained in handling high-sensitivity freight and aware of the importance of securing cargo against movement.
- AIG Marine Risk Consulting HIGH VALUE THEFT TARGETED (HVTT) LEVEL 2 SECURITY should be considered.
- Limit values per truck depending on the risk in the transit area to lower the accumulation risk.
- In addition to the security considerations of route planning, environmental extremes should also be assessed and if necessary, the racks should be shipped in a climate-controlled environment.
- Route planning may also raise concerns with the road conditions, in which case, alternative routes, or speed limits should be mandated.
- If the carrier is not suitably experienced in the shipment of server racks and supercomputers, the presence of an experienced third-party survey is recommended.
- Standard operating procedures should include escalation paths for handling delays, diversion scenarios, or damage events.
- If shipped via shipping container, desiccants should be in place.
- Containers should also be checked before loading to ensure they are watertight with a current CSC approval plate.

For further information, please contact your local Marine Risk Consultant.