Security Breach

Protecting the integrity of pharmaceuticals in the supply chain is a daunting challenge, to say the least. Due to globalisation, pharma companies are put under even more pressure to provide end-to-end security in order to prevent crime and, ultimately, ensure patient safety

Steve Ward
at Pinkerton

Approximately 40% of all pharmaceutical products available in the US are manufactured outside of the country. It is thought that 80% of the active ingredients in drugs are made and delivered from all over the world, and these must meet the country-specific regulatory requirements of the locations in which they are going to be sold. This highlights the complexity of the industry's supply chain.

Like many high-value commodities, pharmaceuticals are attractive to criminals – whether they are online hackers or opportunistic individuals who hijack a truck and remove its goods – with no concern whether they are life-saving drugs, prescription medication or lifestyle products.

Negating threats means thoroughly assessing your entire distribution network to determine penetration points. This can include screening vendors to ensure that they have the proper cybersecurity measures in place; scrutinising physical vulnerabilities along the route where goods can be tampered with; and identifying countries and regions with high risks for disruptions to business continuity that can potentially impact your ability to get products from point A to B.

Global supply chains consist of many working parts: manufacturers, importers, exporters, customs brokers, carriers, consolidators, intermediaries, ports, airports, terminals, integrator operators, warehouses and distributors. You could be forgiven for thinking that it is an impossible job to keep track of security throughout the transit network.

Identifying the Risks

There are, however, security agencies that have the resources to run audits designed to vet and screen personnel, work routines and the cyber and physical infrastructures throughout the entire transit network. Annual audits offer businesses the reassurance that best practices are being adhered to, or will otherwise provide recommendations on how the security of storage and transit of goods can be improved and risk of criminal interception minimised.

A number of pharmaceutical companies have introduced transportation carrier audits of their own, which are risk assessments based on the country and the location the goods will travel through. They work to specific guidelines depending on the product being delivered – for example, a lifestyle product will not necessarily have the same security review as a prescription drug.

Whatever the product, an audit is expected to identify potential weaknesses in the supply chain, which will involve basic security measures such as:

- Personnel assessment
- Confirm the warehouse has a complete and sound perimeter fence
- Ensure the goods stored properly
- Check if there are other products being kept alongside the drugs
- Verify that CCTV is operational and access control installed

Some audits will demand that the product is segregated from others and stored in a temperature-controlled environment, as well as confirming that the logistics operator has the correct regulatory certification for different countries available – such as C-TPAT 2.0 in the US and an authorised economic operator in the UK.

Scrutinising these basic requirements of the distribution process is key to fixing some of the gaps that can occur in supply chain security. Alternatively, third-party providers can offer transportation and cargo audits on a global scale. After all, customers in Europe, the Middle East and Africa may adhere to a company's guidelines but they may be found wanting in the Asia-Pacific region.

Other vulnerability issues for pharma businesses include intentional adulteration of a product by someone with access to the supply chain, cargo theft and mislabelling of goods. Then there are the problems of counterfeit products being passed through a legitimate supply chain and, on the other side, legal businesses unwittingly moving illegal contraband – these can all be linked to slack security.

Addressing the Problems

Workers have a critical role in an organisation's cyber and physical security. They are a company's most important asset – but that same employee could also be one of the biggest risks to a firm's electronic information, physical and human security, as well as a hazard to reputation if not vigorously vetted prior to placement. Comprehensive recruitment screening for pharma organisations is one way of protecting supply chain networks from potentially rogue or disgruntled staff. They may be tempted by fraud, theft or – something that is becoming a significant problem in a number of countries – bribery.

Some companies utilise a risk index, which focuses on individual countries and the perils that area could pose to your supply chain – such as corrupt officials – but also other factors including weather intelligence and the political situation.

Anti-bribery investigation programmes follow along similar lines of supply chain security audits, where stakeholders are thoroughly researched in order to check their backgrounds to discover if they have ever been mentioned in WorldCompliance™ audits. Due to the political climate in certain countries, bribery is almost an accepted method of transporting goods safely through border controls, but organisations can still be hit by massive financial penalties for the practice. Vetting and screening employees of third-party providers for any bribery sanctions, as well as identifying a supplier's anti-bribery policies, can offer crucial knowledge.

Pharma businesses are becoming much more proactive in screening logistics suppliers. However, it is not a procedure that is easily adopted. If you are turning your vetting process over to a security agency, ensure that it not only has experience in the industry, but has thorough knowledge of the supply chain and also understands the laws of world compliance.

Many organisations use a self-assessment form for a third-party logistics provider,

> "It is thought that 80% of the active ingredients in drugs are made and delivered from all over the world, and these must meet the country-specific regulatory requirements"

bespoke to the client's needs. It takes into account many factors, such as the country of origin, whether or not previous audits and employee vetting have been carried out, any fines incurred; it can also check if the company has changed ownership an unusual amount of times over the years. Sometimes, they will neither meet with you nor submit to the audit, which probably makes your decision whether or not to contract an easy one.

The War Online

Cyber intrusion is becoming an increasing menace to pharmaceutical products. The more complex and internet-dependent the supply chain, the more attractive it is for cyber criminals to exploit it – especially if it involves high value drugs – by monitoring, identifying and targeting loads.

Organised criminal operations can and do hack into internal systems to divert consignments of drugs to a less secure facility where they have people on the payroll – allowing those goods to then disappear out the door. Pharma companies need to have a marriage of both information and physical security to minimise this risk of criminal infiltration.

Another scam is for criminals to steal a lorry and set up a fake trucking website, displaying false certification. They can then just wait for a legitimate business to come to them. When they get that call, they drive the vehicle straight in, load up and then drive out again before dumping the truck and making off with the goods. During the investigation into what happened in this instance, it turned out no background checks or screening were performed on the carrier.

Countering the Counterfeiters

The screening of third-party service suppliers is vital. Companies also need to forge a good relationship with law enforcement agencies in the battle against counterfeiting. Offenders seek to capitalise on any weaknesses in the supply chain, from manufacturer to end user – security audits can help close the loopholes that the counterfeiters would so readily exploit.

Flaws in the supply chain appear where counterfeit drugs, or outdated ones that have not been disposed of properly, find their way onto an online market that does not adhere to official regulatory procedures. They also arise where fake products are fed into an established supply chain unbeknown to the original manufacturer. The pharma industry must address these challenges aggressively. Whereas counterfeit jeans may not stir local police into action, counterfeit drugs are treated very differently as law enforcement agencies understand the danger and threat these pose to the community.

You would be surprised how involved agencies and national health ministries are with the pharmaceutical trade in order to combat counterfeiting and to prosecute criminals. Companies should, therefore, cultivate and maintain these levels of collaboration.

Stay Safe

The more remotely we are working, the greater the opportunity for criminals to find a way to hack and access information. They are becoming increasingly sophisticated in their efforts to breach security measures and will take advantage of any chinks in the supply chain to achieve their goals. Pharma companies must make use of every option available to them to guard against the erosion of drug safety and to protect themselves against large economic losses.

About the author

Steve Ward serves as Vice President for the Global Intellectual Property Protection division at Pinkerton, a global provider of corporate risk management services including security consulting, investigations, executive protection, employment screening, protective intelligence and more.

Email: marketing@pinkerton.com