Dangerous liaisons

Despite the global focus on the dangers of systematic and organised crime, the pharmaceutical industry has revealed itself to be vulnerable to acts of terrorism. **Dr Miri Halperin Wernli**, **Dr Boaz Ganor** and **Mollie Shields-Uehling** reveal the steps that the industry should take to minimise risks to staff, products and patients.

Dr Miri Halperin Wernli
Dr Miri Halperin Wernli is vice-president, deputy head global clinical development, and head of global business and science affairs at Actelion Pharmaceuticals (Basel, Switzerland). She has over 25 years' experience in healthcare and pharma.

In the decade since 9/11, the US Government has implemented a series of post-attack procedures, policies and technology upgrades that have intercepted large and small terrorism attempts.

Today, the global pharmaceutical industry is reacting to a series of incidents that have exposed equivalent vulnerability.

The most devastating are instances of economically motivated adulteration (EMA), the clandestine substitution of dangerous but cheaper chemicals that will test correctly in incoming assays. EMA has resulted in thousands of documented deaths. Arguably, the relabelling and distribution of stolen and diverted low-dose biopharmaceuticals has been almost as devastating.

> "Pharma needs to concentrate on strategies that close off two kinds of risks: 'front door' (where pharma has control) and 'back door'."

Industry reactions to these challenges tend to focus on trying to close the potential for criminal, not terrorist, exploitation. Pharma is inclined to place security efforts on protecting products after they leave manufacturing – and then, only against those with criminal intent.

A strong case can be made to say that industry has inadequately focused on how those with terrorist intent might

gain employment in pharma company or vendor laboratories. It has insufficiently monitored those with access to, or knowledge of, how to defeat inadequate industry security to steal lethal chemicals, toxins, organisms or technology, or to contaminate products manufactured there. Most likely, there is little or no security against those who might gain entry to manufacturing, storage or distribution – not to steal product, but to substitute contaminated solid or liquid counterfeits containing lethal compounds. Such potential terrorist infiltration might appear so improbable or remote that specific protective measures are unnecessary. In retrospect, so did the possibility of multiple hijacking of aircraft on 9/11.

Those who might exploit pharma weaknesses include domestic and international terrorists (networks and lone wolves), anarchists such as anti-globalism activists, doomsday cults, environmentalists, animal rights activists, and groups and individuals with a political grudge.

> "Employees who leave with specialised terrorism-valued knowledge should be systematically followed and reported if they 'fall off the radar'."

Areas of vulnerability

Pharma needs to concentrate on strategies that close off two kinds of risks: 'front door' (where pharma has control) and 'back door' (where pharma does not have direct control). These risks could be related to a variety of factors all along the pharma chain, from its people and their specific knowledge and expertise, to the materials in its research laboratories and the potential that its products as well as its manufacturing and distribution systems and channels could be breached by criminals and terrorists. Front door risks include:

- **Inadequate personnel-background checking prior to hiring individuals who will have, or could obtain, access to technology, materials, equipment or training of potential use to terrorists.** Today, many pharmaceutical companies perform routine reference checking on CVs, mostly confined to previous employment. Without appearing intrusive, they try during face-to-face interviews to detect any evidence of potentially antisocial behaviour. Some may submit applicant names to internet search engines to detect any associations, blogs or social network comments that raise concerns. Inadequate reference checking can occur even in the most secure government facilities, as seen in the US anthrax-letter incidents in which government employees were found to have falsified their background information.
- **Inadequate continuous investigation and monitoring of staff scientists and engineers with specialised pharma know-how and purchasing responsibilities.** Disaffection and/or vengeance on company products or colleagues can arise over resentment for a reprimand, having a favourite programme cancelled, a patent or paper submission refused, or being passed over for promotion. Psychological problems can surface because of alcohol or substance abuse, financial and other personal problems. Vulnerabilities due to family members living in high-threat nations, or sexual orientation, can subject an employee to blackmail threats and other external pressure. As a result, they can be exploited or recruited by a terrorist organisation, even after leaving the company. Unauthorised purchases are another way employees may abuse their authority to obtain terrorism material or equipment. Suppliers to research laboratories should expect to receive purchase orders only on standard, controlled forms so that no employee could order biologicals using company letterheads.
- **Inadequate protection of sensitive facilities (manufacturing and packaging) and of materials and equipment with terrorism potential.** To assure optimum protection, pharma must imagine how employees could abuse their security clearance to obtain materials, organisms or chemicals of terrorism value. Late-night laboratory workers could misuse access to organisms and equipment with potential terrorist use – the suspicion behind the US anthrax attacks.

Boaz Ganor
Boaz Ganor is Ronald Lauder chair for counterterrorism. He is also the founder and president of the International Academic Counter-Terrorism Community, an association of academic institutions, experts and researchers related to the study of terrorism and counterterrorism.

Back door risks include:

- **Infiltration of the supply chain by unreliable vendors.** Economically motivated adulteration represents a potential new industry bioterrorism risk. Whether by accident or indifference, those who perpetrate EMA have killed many. Individuals seeking to infiltrate global pharmaceutical production and distribution could easily insert assay-resistant compounds into a pharmaceutical company's manufacturing to sicken or kill large numbers of people. Unfortunately, the nations that harbour EMA violators rarely criminalise them. Another variant of unreliable-vendor risk arises when validated suppliers silently subcontract to unvalidated vendors, often manufacturing in countries with questionable regulatory controls.
- **Infiltration of the distribution chain, including transport, warehouses and wholesalers.** For decades, theft of prescription pharmaceuticals was treated largely as a property crime. Today, those thefts are recognised as representing a significant risk to public health – and they signal avenues that terrorists could exploit to introduce lethal preparations into the system.
- **Infiltration of counterfeit medicines.** The widespread infiltration of counterfeit prescription and over-the-counter products represent more than an economic or even general health risk – they represent a potential avenue for terrorism. Criminal groups worldwide have perfected techniques of manufacturing and packaging counterfeits visually indistinguishable from authentic brands. They have

also mastered the technique of inserting counterfeits into wholesaling and retail channels where assays would be rare. Terrorists could exploit these same technologies to inflict illness, death and fear among prescription and non-prescription drug consumers. Counterfeits represent not only an important public health hazard, they are also a national/international security threat. The links between counterfeit goods and terrorists have been well established. Today, terrorists seem to prefer the 'shock and awe' of explosives to spread fear among target populations; however, the same technology and security gaps that criminals use to put counterfeit drugs into retail drugstores could be exploited to place deliberately toxic medications into widespread distribution, with potentially horrific effect.

> "Pharmaceutical companies should unite with top drug chains and wholesalers against renegade purchases from intermediaries."

Suggested measures to monitor and counter the risks

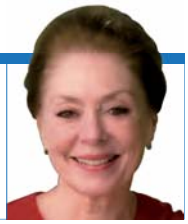
There are several ways that risks can be monitored and countered; for example, enhancing the control and monitoring of all critical staff prior to hiring, during employment and after leaving. All staff in sensitive positions that expose them to organisms or technology of potential application to terrorism should:

- implement systematic background checks prior to recruitment. Background investigations should at least include verifying an individual's references and checking government databases for criminal history or links to terrorist organisations.
- implement ongoing monitoring and periodic reinvestigations. Monitoring and periodic reinvestigations should be routine because problems may arise long after the person has been hired. Reinvestigation is indicated before a staff scientist is granted unescorted access to secure areas.
- take note of critical employees who depart without notice and leave no contact information. If the employees had contact with organisms or technology with terrorism potential, government security organisations should be alerted.

Recognise the 'terrorist value' of specialised pharma know-how and technology. Terrorists have attempted to use a variety of infectious organisms for terrorism – anthrax, botulinum toxin and salmonella. In almost every case, few or no deaths resulted because the terrorists lacked the expertise needed to aerosolise and disperse those agents. Thus, aerosol expertise would be most valuable to terrorists, because past biological attacks were limited by that technology. Employees who leave with specialised terrorism-valued knowledge should be systematically followed and reported if they 'fall off the radar'.

Efforts should be increased to secure facilities, materials and equipment with potential terrorist use against theft or misuse. Adopt a much more integrated approach to biosecurity: a combination of physical protection, access controls, materials accountability and personnel screening. Closely monitor/guard all biological and

Mollie Shields-Uehling
Mollie Shields-Uehling is president and CEO of the SAFE-BioPharma Association. She directs the business and strategic activities of the association, and is a member of the board of directors. She has over 20 years' international trade and biopharmaceutical industry experience.



chemicals assets with potential terror use and intensify screening of all raw materials received.

- Carefully account for pathogens during storage and experiments.
- Conduct inventories and audits of all sample collections.
- Apply 'chain of custody' outside access-controlled areas.
- Destroy and account for all working stocks at the end of experiments.
- Carefully secure any equipment of potential terror use, including its disposal.
- Intensify screening of every batch of new raw materials received.
- Assume that suppliers may switch vendors and subcontractors without disclosing them – even when receiving shipments from FDA-validated international suppliers.
- Adopt new technologies, such as energy dispersive X-ray diffraction, which can remotely analyse the crystal structure of material through plastic, cardboard and metal packaging.

Treat theft and counterfeiting as seriously as deliberate introduction of toxins. To reduce risk, pharmaceutical companies should unite with top drug chains and wholesalers against renegade purchases from intermediaries. Optimally, all will establish industry-wide encrypted track and trace identification of pharmaceuticals across the supply chain with an electronic drug pedigree – an 'ePedigree'. Such a validation would document a drug's origin as well as each prior sale, purchase or trade of a drug. It would include the dates of transactions, as well as names and addresses of all parties involved in the transactions. The ePedigree would contain a digital signature created via only government-approved technology and verified by an automated system.

Introduce the use of interoperable digital identity technology to assure greater trust in online identities. The pharma industry relies on the internet to facilitate global collaboration. Digital identities compliant with the SAFE-BioPharma standard mitigate risks inherent in these electronic transactions. It does this by providing standardised ways to manage and verify digital identities and to apply legally binding digital signatures to electronic documents. Each identity is closely bound to the actual, proven identity of the individual to whom the credential is assigned. Use of these digital identities can be applied to a broad variety of functions and purposes, from applying legally binding signatures to cloud-based clinical trial documents and authenticating into clinical portals, to signing chain-of-custody documents.

Time for action

New and different challenges caused by terrorism need to be recognised and addressed by the global pharmaceutical industry. They apply both to lone wolves and large organised terrorist groups.

By understanding the described potential gaps and the associated risks, and by taking the recommended measures, pharma can prevent or minimise the possibility of potentially severe consequences for the public and the industry. ■