Pipeline of Terror

As the knowledge of manufacturing drugs and the processes behind it increase, the industry could be leaving itself wide open to a potential terrorist attack if proper security controls are not implemented

Boaz Ganor, Miri Halperin Wernli and Mollie Shields Uehling

Isn't it ironic that an industry dedicated to improving health could become a vehicle to deliver destruction? That is the unfortunate reality of the global biopharmaceutical industry. Without proper controls in place, our pipeline could easily become a pipeline of terror.

Numerous security experts consider it's only a matter of time before determined rogue groups create havoc by exploiting the vulnerabilities of a partially secured industry. Without wishing to be sensationalist, over the past few decades, the number of people with knowledge of bioengineering processes has increased dramatically, potentially providing terrorists with a skilled 'bio-weapon' production workforce.

Dangerous pathogens and biological toxins – such as botulinum toxin, ricin, tetradotoxin and conotoxin – are present in private research laboratories worldwide. The firewall between their therapeutic and terroristic uses is inadequate, and could have disastrous consequences.

To minimise the risk of the biopharmaceutical industry becoming a mechanism for terrorism activities, it needs to be alert to these possibilities and take mitigating action.

Industry Disruption

Daily headlines have trained us to associate global terrorism with well-defined groups such as Al Qaeda and Hezbollah. These and their counterparts are high on the list for disrupting the industry by undermining drug integrity, introducing counterfeits and substituting lethal materials for legitimate ingredients.

We have seen this repeatedly. Iran has sophisticated drug manufacturing capabilities and well-trained personnel. The US Drug Enforcement Agency recognises that Hezbollah and Hamas make counterfeit medicines which are distributed via criminal networks throughout the Middle East and Latin America. Their significant profits are 'reinvested' into the groups' terrorist activities.

Terrorism is not limited to the obvious. Domestic groups can be part of the equation. Every company with a vivarium understands the potential of disruption from animal rights activists, and most have prepared for this with physical security and changes in testing policies.

Recent anti-globalisation initiatives may extend their actions well-beyond Davos and the G8 Summit. Will they do more than demonstrate? Economies that no longer provide the young with opportunities can produce people who choose to act out against wealthy companies and their leaders.

A troubling picture of this type of behaviour – fictionalised, but very much possible – is presented in the

Image: No 1371, www.freerangestock.com

recent film, *The East*, in which a small group of well-bred urban terrorists take on untouchable polluters and other companies. Their treatment of a pharmaceutical company is disproportionate to the company's alleged misdeeds. This is a current example of popular culture's vilification of the term 'pharmaceutical company'. As an industry, we are subject to bias when it comes to almost everything, except the benefits that our products deliver.

Learning Curve

Kidnappings, hijackings, occupation of remote energy production facilities and cyber-attacks have caused industry executives to begin to shift their thinking from criminal action to terrorist exploitation. This shift in thinking also brings a sharp learning curve with it, based around identity and security considerations.

Because we function in a vulnerable environment, the industry needs to do everything it can to establish a trust framework for its information and human resources. Trusting cyber identities in internet transactions is critical to the safety of every aspect of drug discovery, development, manufacturing and distribution.

Long-established human resources screening, monitoring and other processes are inadequate protection against determined rogue groups and networks that are set on co-opting people and materials for terrorist purposes. They may also miss the trusted scientist or technician who, because of disappointment, disillusionment or political shift, becomes a 'lone wolf', capable of individual mischief or becoming a clandestine terrorist recruit.

Identification Policies

Human resources and information security executives within pharma need to review policies in light of the following:

Background Checks
Understanding the human resources that staff laboratories' manufacturing and distribution facilities is a priority in the fight against potential terrorist activities. These individuals may have access to technology, materials, equipment or training with terrorist potential. Are routine reference checks and in-person interviews adequate protections?

Given the sensitivity of the potential for terrorism, these traditional screening approaches need to be re-thought and re-tooled to include psychological screening for paranoia; narcissism; anger issues; online searches; checks of public records for evidence of instability and arrest; and review of claimed publications, patents and other intellectual output for credibility and plausibility.

Ongoing Investigation and Monitoring
Staff scientists and engineers with specialised pharma skills who hold purchasing responsibilities are in roles that can easily be turned against the organisation. This may come in the form of payback for a reprimand, cancellation of a favourite programme, refusal of a patent or paper, or being passed over for promotion. Alcohol or substance abuse, financial and other personal problems, family members living in high-threat nations, and sexual orientation are among factors which could subject employees to blackmail threats and exploitation and/or recruitment by a terrorist organisation. Companies also need to be alert to unauthorised purchases that, unbeknown to the employer, may be diverted for nefarious use.

Standardised Cyber Identities
Internet communications have helped the pharmaceutical industry achieve new levels of globalisation and collaboration. However, this operating environment creates trust issues in the identities of those both inside and outside of the firewall to whom we provide access to valuable intellectual property and other information assets.

SAFE-BioPharma standardised and interoperable digital identities provide high-assurance trust between parties engaged in secure internet transactions. They are used to authenticate the true identity of the person seeking access to protected information assets, and also improve how all documents are signed by providing digital signature capability, which protects the document from any future changes and verifies the identity of the signatory. Each identity is closely bound to the actual proven identity of the person to whom the credential is assigned. The user only needs one credential for use with all the partners, as opposed to a different digital identity for each one.

No policy or procedure can fully eliminate the threat of terrorist infiltration of an organisation or exploitation of its resources, but the use of standardised digital identity credentials significantly and efficiently reduces risk through the use of sophisticated cryptographic technology.

Integrated Security

Many companies continue to use outdated twentieth century techniques

“Kidnappings, hijackings, occupation of remote energy production facilities and cyber-attacks have caused industry executives to begin to shift their thinking from criminal action to terrorist exploitation”

in an era of new security challenges. The industry needs to embrace a more integrated approach to bio-security that combines physical protection, access controls, materials accountability, personnel screening and information security.

Paying More Attention

How could employees with a terrorist agenda abuse their security clearance to obtain materials, organisms or chemicals? We know of attempts to use infectious organisms, such as anthrax, botulinum toxin and salmonella, for terrorist purposes. Fortunately, lack of know-how about 'weaponising' has limited their deployment, but for how long?

Integrating bio-security by properly safeguarding and keeping an inventory of all biological chemicals and equipment with terror potential is essential, as is applying 'chain of custody' protocols outside of access-controlled areas. The use of biometric devices to access lab servers and restricting remote access to these are important considerations. An intelligent policy based on clear thinking can help to avoid bio-terrorism events.

Supply Chain Security

Economically motivated adulteration (EMA) – deliberate, accidental or the result of indifference – has caused thousands of fatalities. How difficult is it for a terrorist group to infiltrate a production or distribution facility and insert assay-resistant compounds that affect large numbers of patients? EMA violators are harbored in nations that rarely criminalise their actions. Complicating this problem is the occasional practice of validated suppliers subcontracting to unvalidated vendors who may carry out manufacturing in countries with mild regulatory controls.

Distribution Chain Security

For most companies, prescription drug theft is viewed as property crime. Governments view such incidents as a public health risk. Smart minds in the security and anti-terrorism communities now consider the distribution chain – transport, warehouses and wholesalers – to be an accessible route for the introduction of lethal materials. It is precisely this situation that caused US over-the-counter drug makers to introduce tamper-resistant packaging in the 1980s.

Counterfeit Medicines

The proliferation of counterfeits is also an easy entry point for drug terrorism. Worldwide, criminal groups have perfected manufacturing and packaging counterfeits that convincingly imitate the real thing. Unfortunately, these false products have been slipped into legitimate wholesale and retail channels. Is it a matter of time before terrorists utilise this frightening model to inflict illness and death? The damage, fear and disruption of routine living could be impacted as dramatically as that from September 11th.

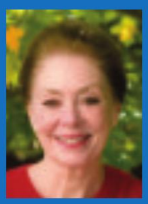
Taking Action

The biopharmaceutical industry houses knowledge and technology that, when placed in the wrong hands, can be used by terrorists to achieve political, economic and religious goals. This poses new and different challenges that need to be recognised and addressed by company decision-makers, security agencies and the global pharmaceutical industry. Starting within our companies, management responsible for security, human resources, information technology, R&D and manufacturing must understand the potential gaps and associated risks, and at the very least adopt these recommended measures. By doing so, the pharmaceutical industry can prevent or at least minimise the possibility of potentially disastrous consequences. We know it is on the terrorist agenda. It is now essential that it is on ours.

About the authors

Dr Boaz Ganor is the Deputy Dean and the Ronald Lauder Chair for Counter-Terrorism at the Lauder School of Government, Diplomacy and Strategy, founder and Executive Director of the International Institute for Counter-Terrorism, and Head of the Counter-Terrorism and Homeland Security Studies Programs at the Interdisciplinary Center, Herzliya, Israel. Boaz is also the founder and Chairman of the International Academic Counter-Terrorism Community. He has published widely used books on terrorism and counter-terrorism and his textbook, *The Counter-Terrorism Puzzle – A Guide for Decision Makers*, is used in universities worldwide. **Email: ganor@idc.ac.il**

Dr Miri Halperin Wernli is Vice President, Deputy Head, Global Clinical Development and Head of Global Business and Science Affairs for Actelion Pharmaceuticals. She has more than 25 years of clinical development experience in the pharmaceutical industry, and in biomedical and medical device early technology research. Prior to joining Actelion, she held global managerial positions in R&D and strategic marketing at Merck, Sharp & Dohme and Roche Pharmaceuticals. **Email: miriam.halperin_wernli@actelion.com**



Mollie Shields Uehling directs the business and strategic activities associated with the global SAFE-BioPharma digital identity and digital signature standard. She has more than 20 years of international trade and biopharmal industry experience. Mollie headed an international public affairs consultancy and served in various leadership positions with Bristol-Myers Squibb, Wyeth, the International AIDS Vaccine Initiative, the White House Office of the US Trade Representative, and the US Foreign Commercial Service. She has been recognised by *PharmaVOICE* as one of the pharma industry's most influential leaders. **Email: mollie.shields.uehling@safe-biopharma.org**