Life Science Leader
January 2014

Pharma Business

Pharmaceuticals: Target For Terrorism

By Dr. Miri Halperin Wernli and Dr. Boaz Ganor

Slowly and steadily, terrorism, like a malignant cancer, has entered our lives. What once was an occasional event on the other side of the world can no longer be ignored as someone else's problem. Terrorists, alone, in cells, or part of expanding international networks, are affecting the way we live, the way we think, and the way we do business. Government facilities, planes, trains, ships, oil refineries, and luxury locations have all taken the biggest and most publicized hits.

The biopharmaceutical industry has seen it in the form of counterfeiting, adulteration, and diverted product, all of which are, perhaps, more disruptive than destructive.

But that can easily change. The ingredients, technologies, knowledge, and global distribution inherent in making and delivering medicines can be turned too easily from benefit to destruction. That's why we, a senior pharmaceutical executive and the head of a counterterrorism think tank, wrote this article. It is part of an ongoing initiative to explain why the biopharmaceutical industry needs to be alert to its vulnerabilities to terroristic influence and what it can do to reduce the risk.

WANING PUBLIC SUPPORT FOR BIOPHARM

Fundamental to understanding the problem is an understanding of the origins and motives of those who would do harm. It's a fellowship of strange bedfellows: people from different backgrounds and with different agendas willing to deploy extreme violence to send their messages and to get their way. What they have in common is the use of violence among other tactics to impose their will.

We also need to appreciate the cultural environment in which the drug industry exists. The negative image portrayed in popular media shapes how people think. There was a time when the industry was held in high regard by most levels of society. That has changed, and life-saving or life-enhancing benefits aside, there's little understadning within the general population of the way drugs are developed, marketed, and sold. A recent opinion survey of 600 international, national, and regional patient groups on the corporate reputation of pharma in general and 29 leading pharma companies in particular indicated that only 34 percent of respondents gave pharma a "good" or "excellent" rating. Among the areas patient groups rated pharma as having a "poor" record were 1) a lack of fair pricing policies leading to unseemly profits (50 percent); 2) a lack of transparency in all corporate activities (48 percent); 3) management of adverse event news (37 percent), and 4) acting with integrity (32 percent).

For a business concerned with health, such waning popular support creates an unhealthy reality. The biopharmaceutical industry is highly vulnerable. In response, industry executives need to expand their security thinking to protect against terrorist exploitation.

BANKROLLING TERRORISM WITH COUNTERFEITS

The US Drug Enforcement Agency recognizes that Hezbollah and Hamas make counterfeit drugs that are distributed and sold by established criminal networks throughout the Middle East and Latin America. This trafficking produces revenues that fund their terrorist activities.

They aren't alone. Other terrorist and criminal groups trade in counterfeits. It's a low-cost, high-margin business preying on a voracious market being robbed of the therapeutic benefits of the real thing.

As if the use of counterfeits to bankroll terrorism were not bad enough, think about the mass damage a zealot or other madman could cause by adding a lethal ingredient to these so-called drugs. Memory of the still-unsolved Tylenol killings in the Chicago area haunt those who recognize just how vulnerable unprotected pipelines can be.

TERRORISM RECEPTOR SITES

The equipment, materials, and personnel on which industry relies are potential terrorist targets. Laboratories, equipment, and other facilities that could be used to manufacture deadly pathogens are spread across the globe: the hospital in Karachi, the university chemistry lab in La Paz, the clinical research site in New Delhi.

Botulinum toxin, ricin, tetradotoxinm, conotoxin, and other deadly toxins already are present in many private-research laboratories. Is the security keeping them from us any more than a key to the front door and knowledge of what might be found in the fridge?

And, perhaps most significant, there is an ample supply of personnel trained to understand bioengineering processes. A 2009 WHO survey identified 466 biomedical and clinical engineering teaching units in 90 of its member states. That comprises a global educational infrastructure that has produced engineers, technologists, technicians, and assistants in the tens of thousands, if not more. There is no lack of talent that, with the right incentive or intimidation, could be redirected to harm.

The industry will never have total control of these risk factors, but it can take measures to minimize them. Toward this end, we have grouped security risks into “identity” and “security.”

IDENTITY

Establishing a trustworthy framework for information and human resources is an essential first step in minimizing, if not preventing, the effects of insidious forms of terrorism.

Cyber-Terrorism

Use of the Internet for global collaboration opens the possibility that those we rely on are not who they present themselves to be. This possibility of cyber-terrorism masked as false representation can compromise drug discovery, development, manufacturing, and distribution by allowing the wrong people access to valuable intellectual property and other information assets.

Mitigating this risk is possible through the use of standardized digital identities. The global SAFE-BioPharma digital identity standard was developed by the industry and regulators, such as the FDA and EMA (European Medicines Agency), to provide high-assurance trust between parties engaged in secure Internet transactions. Many companies already are members of the nonprofit that manages the standard, and its IT, HR, and security groups can utilize its sophisticated cryptographic technology to guard against unauthorized access to protected information.

UPGRADING HR PROCEDURES

As vulnerable as IT may be, human resources is even more exposed. Conventional screening techniques are inadequate to reveal bad actors intent on infiltrating an organization for the wrong reasons. And how often are existing — especially long-term employees — monitored without prejudice because of longevity or internal political alliances? History is littered with turncoats who have been denied promotion or whose pet projects have been defunded.

We recommend that HR executives re-examine background-checking protocols, especially in the terrorist-vulnerable areas of laboratories, manufacturing, and distribution. The access to technology, materials, and equipment should make careful screening of personnel staffing in these areas a priority. Routine reference checks and in-person interviews should be supplemented with psychological screening for personality disorders such as paranoia, narcissism, and anger management issues. There should be deep online searches, including checks for public records of instability and/or arrest. And CV-enhancing claims of publications, patents, speaking engagements, and other professional accomplishments should be carefully reviewed for plausibility and credibility.

Also recommended is a policy of ongoing personnel investigation and monitoring, especially of staff scientists and engineers with specialized pharmaceutical skills and purchasing responsibilities. They occupy roles that, given the right circumstances, can be turned against their employers. Common scenarios include retribution for cancellation of a favored program, a reprimand, refusal of a patent or paper, or losing a promotion. Issues less visible to management, but potentially exploitable by a terrorist organization, are alcohol or substance abuse, financial and other personal problems, sexual orientation, or family members living in high-threat nations. The determined terrorist will use blackmail to leverage these situations for access to equipment and expertise or to divert materials or to force the unauthorized purchase of critical substances.

SECURITY

Traditional brick-and-mortar security is needed in every industry. But new challenges require biopharmaceutical industry security executives to embrace a fully integrated approach, combining physical protection, access controls, and materials accountability. Combined with the information security and personnel screening described earlier, these will strengthen the company’s physical and cyber perimeters.

We strongly advise biometric devices as part of the protection of laboratory and other facilities housing materials and equipment, and servers. We also recommend ongoing inventorying and proper chain-of-custody protocols for all terror-prone biologicals, chemicals, and equipment outside of access-controlled areas.

PROTECTING THE SUPPLY CHAIN FROM ADULTERATION AND COUNTERFEITS

Economically motivated adulteration (EMA) — the adulteration of ingredients — has resulted in widespread misery and loss of life. While deaths have generally been in the hundreds, sophisticated terrorists infiltrating a production facility and introducing assay-resistant toxic ingredients could alter that calculus dramatically.

This is no idle concern. In 2007 and 2008, dozens of U.S. patients experienced adverse events from heparin that had been adulterated while being manufactured in China. In 2009 a shipment of more than 125,000 vials of insulin was stolen and stored in unknown conditions before being sold to pharmacies and patients. And 115 Panamanians died from ingesting cough syrup in which cheap diethylene glycol had been substituted for more expensive glycerin.

Manufacturers need to adopt electronic pedigree techniques to track and trace drug ingredients. They also need to advocate more direct action by the FDA and other regulatory bodies.

The counterfeit problem is more severe. According to the Center for Medicine in the Public Interest, sales of counterfeit drugs are around $75 billion and growing rapidly.

SECURING THE FUTURE

It's said that awareness is the first step toward change. Growing numbers of pharmaceutical decision makers are becoming aware of the problems discussed in this article. More attention needs to be directed to hiring and personnel monitoring practices. Scrutinizing online identities needs to be standardized with sophisticated cryptographic technologies. Terrorist groups already are counterfeiting drugs and distributing them through criminal cartels. The industry needs more initiatives to identify bogus drugs and to inform pharmacy professionals and consumers of ways to avoid and/or detect them. Of greatest concern is the potential for terrorist groups to expropriate criminal cartel resources and turn them from a source of income to a form of targeted destruction.

Sales from counterfeit drugs are around $75 billion and growing rapidly.

The technologies to prevent that doomsday scenario will evolve. For now, companies need to be aware of the problem, take practical action, and remain vigilant. It is a matter of corporate — and public — health.

About the Authors

Dr. Miri Halperin Wernli is VP, Deputy Head of Global Clinical Development, and Head of Global Business and Science Affairs at Actelion Pharmaceuticals.

Dr. Boaz Ganor is deputy dean and Ronald Lauder chair for counterterrorism at the Lauder School of Government, Diplomacy, and Strategy. He is also founder and executive director of the International Institute for Counter-Terrorism (ICT) and the head of the counterterrorism and homeland security studies programs at the Interdisciplinary Center (IDC) in Herzliya, Israel.

Dr. Miri Halperin Wernli
Vice President, Deputy Head of Global Clinical Development
Head of Global Business and Science Affairs

Actelion Pharmaceuticals Ltd
Gewerbestrasse 16
CH-4123 Allschwil
Switzerland
email: miriam.halperin_wernli@actelion.com