

Getty Images/Jeffrey Hamilton

Dangerous Liaisons



How vulnerable is Big Pharma to the predations of organized terrorist groups or that rogue malcontent with an agenda to wreak havoc on society? Two international security experts say it may only be a matter of time—and that the best protection against that vulnerability is vigilance.

By Miriam Halperin Wernli and Boaz Ganor

The US commission studying the September 11, 2001 Al Qaeda attack on New York and Washington concluded that America's vulnerability resulted from a "failure of imagination"—specifically, a failure to envision the improbable but possible use of hijacked airlines as weapons of mass destruction. To date, no pharmaceutical company's scientists or technology have been traced to a domestic or international act of terrorism. Yet despite the absence of any documented attempt to exploit gaps in current pharma security via direct or cyber-based subterfuge, we have analyzed the risks and are prepared to caution the industry against at least three

other "failures of imagination"—even if they appear unlikely today. These are:

- » The potential for terrorists to steal via cyber-theft confidential proprietary technology or materials directly, or through contracted surrogates.
- » The potential for a disgruntled or blackmailed employee—or a new employee who has been inadequately screened—to exploit opportunities from within a company to introduce toxic contaminants into the final production stages or packaging of medicines or vaccines.
- » The potential for terrorists to gain access to pharmaceutical and biologic

technology and apply it in such a manner as to inflict chemical or bioterrorism indiscriminately, placing thousands—even millions—of people at risk.

US drug supply: The weak link

For decades, the production and sale of fake drugs were largely confined to the third world; the danger was mostly to solid dosage forms. Recently, fake solid and injectable brand drugs have penetrated the industrialized economies, exposing both the industry and its customers to more risks than might meet the eye.

» Chronic shortages of generic injectable drugs have driven gray market prices up by thousands of percent—making them, for the first time, candidates for potential counterfeiting. Counterfeiters today may feel they have even greater latitude in picking from a whole panel of short-supply injectables, due to the shortages of many very basic drugs and their less

complex generic labels and packaging. The potential “market” for fakes of generic injectable drugs extends to thousands of hospital and clinics—covering even more territory than the brand injectable drugs they’ve counterfeited to date.

- » The FDA has discovered fake injectable brand drugs in United States hospitals and clinics. First to appear were fake Procrit and Epogen, then fake Avastin. Some of these fakes originate with domestic criminals; others with as-yet unidentified foreign manufacturers.
- » Beyond the fake erectile-dysfunction and narcotic drugs sold on the Internet, investigators have found in US pharmacies near-perfect truly counterfeit Lipitor tablets containing atorvastatin, packaged along with diverted overseas-manufactured tablets of the genuine drug, assembled in counterfeit dose packs.
- » Baxter’s tragic experience with long-trusted Chinese suppliers of heparin precursor—the substitution of that key ingredient with a toxic chemical was designed to fool the incoming US factory assay—demonstrated the vulnerability of both brand and generic companies to overtly criminal economically motivated adulteration by overseas vendors in their raw materials supply chain.

These criminal exploitations of gaps in the US drug system have been noted by terrorist groups and rogue states. A “failure of imagination” could result from companies failing to consider how committed criminal, political, and terrorist groups might seek to exploit gaps in their employment screening, computer networks, or supply chains to insert fake versions—even toxic fakes—into their distribution channels.

- » The global pharmaceutical industry has been specifically targeted by the leftist international hacking organization “Anonymous,” whose sympathies appear closely allied with those of violent animal rights groups that

have targeted pharma in the past, and with terrorist organizations known to finance their activities through the sale of counterfeit amphetamine Captagon and fake Western drugs.

- » Hackers of unknown origin or intent have successfully penetrated the computer networks of Pfizer, Abbott, and Boston Scientific. Those penetrations may have lasted a month or more until discovered.

Hezbollah, hamas, and Iran have developed their own hacking teams, with evidence that they operate both alone and with the assistance of Russian criminal gangs.

- » Criminals hacked into the computers of America’s largest security company, ADT, obtaining vital security data from companies which was then used to break in and steal from their warehouses and trucks. One of their targets was a drug supply warehouse for Eli Lilly, from which they stole \$75 million in inventory covering a wide range of drugs. Other companies whose drugs were stolen and then resold include Glaxo SmithKline and Novo Nordisk, as thieves targeted both warehouses and long distance trucks.
- » The stolen Novo Nordisk cargo was insulin, which other criminals then sold to small distributors who resold it to the giant Kroger pharmacy chain, which inadvertently bought it even after an FDA warning. Fortune magazine claimed one patient in Ohio who took the insulin went into convulsions; another, in Texas, saw his blood sugar spike.
- » Counterfeit Avastin manufactured in the Middle East penetrated both

European and United States gray-market distribution, and was discovered being administered to patients—after passing through the lawless conflict-zone in Syria.

- » Middle East terrorist factions of Hezbollah and Hamas have been cited by the US Drug Enforcement Agency as manufacturing millions of dollars annually in counterfeit prescription drugs and amphetamines and selling them through criminal networks, both in the Middle East and Latin America. Nineteen Hezbollah operatives in Michigan who ordinarily specialized in dealing in untaxed cigarettes, were indicted in 2006 by a Federal grand jury for trafficking as many as 50,000 counterfeit Viagra tablets into the United States from Canada, and transmitting proceeds from their operations to Hezbollah. Four years earlier, the DEA discovered a similar operation smuggling large quantities of pseudoephedrine from Canada—destined for methamphetamine manufacturing in the Midwest and Mexico, with profits going to Hezbollah.
- » Hezbollah, Hamas, and Iran have developed their own hacking teams, with evidence that they operate both alone and with the assistance of Russian criminal gangs. Hezbollah took responsibility for having hacked into the networks of the US banking giant Wells Fargo. Bank of America and CitiBank have also been hacked.

Pharma’s HR department: A potential gap in corporate security

The 2001 “Amerithrax” anthrax letter attack uncovered gaps in Defense Department screening of scientists with access to dangerous substances, and management’s inadequate monitoring of changes in employee personality due to potential triggers.

The anthrax-containing letters sent to the Senate were traced to lone-wolf

defense scientist Bruce Ivins at the Army's Fort Detrick research labs. Ivins is believed to have begun mailing his letters because of his anger at loss of funding for a research project. So respected was Ivins that he was assigned by the Department of Defense to assist the FBI in seeking the anthrax-letter terrorist—and for months, actually sent investigators in wrong directions.

What should trouble pharma HR is that Ivins' credentials and experience would have made him a candidate for a top research position at just about any global drug company where he might have applied for employment. Ivins' managers failed to take note of personality traits that might have tipped them off that something was wrong, especially after his anthrax vaccine was placed on a development back burner. Management might have detected is-

ssues brought to the attention of the FBI by a former university colleague that he had persistently harassed for years. In fact, Ivins had performed poorly on psychiatric tests, but the results weren't followed up.

Unchecked CVs

Equally troubling to pharma HR should be the multiple mistruths in the CV of Steven Hatfill, the scientist falsely accused of being the originator of the anthrax letters. When reporters began researching Hatfill, they uncovered multiple academic degrees and honors he had never received. All these claims should have been verified before Hatfill was given access to some of the nation's most virulent organism stores.

What should not be missed by pharma HR is that someone with a profoundly falsified CV did gain

access to laboratories where his incompetence could have endangered coworkers and the nation. Resumes for those with such potential access must be rigorously examined, and all claimed degrees, published papers, and experience validated.

Dangers for support staff

In February, armed thieves disguised as police broke through the perimeter fence of the Brussels airport and stole more than \$50 million in gems from the cargo hold of a airliner about to take off. The security gaps that enabled such a precise theft appear to have been guided by inside information by airport personnel. Following the Brussels theft, an airline security specialist made observations about airport security that may merit considerations for possible parallels for pharmaceutical companies:

Flexible Function Space in the heart of Boston's Longwood Medical Area



The Inn at Longwood Medical is the only hotel within 100 yards of Harvard Medical School, Dana Farber Cancer Institute, Beth Israel Deaconess, Joslin Diabetes Center and Brigham & Women's Hospital, and is connected to Children's Hospital Boston.

**Call today for 50% off Meeting Room Rental
AND a \$50 Visa Card for a summer meeting!**



© 2013 Google



The Inn
AT LONGWOOD MEDICAL

Contact us at salesinfo@innatlongwood.com

342 Longwood Avenue | Fenway Kenmore
Boston, MA 02115 | Phone: (617) 731-4700
www.innatlongwood.com

“Ground crews are largely unseen by the general public. But in much the same way as flight crews, they have intimate knowledge about their work environment. They also have unrestricted access to the exterior and interior of aircraft. Despite this access, these employees are not subject to the same security screenings as passengers and most flight crews.”

The Brussels incident suggests the industry needs to consider tighter screening of all who enter their facilities, including those who clean premises—both offices and labs. Many such functions are outsourced to companies paying minimum wage, and—despite blanket assurances and signed commitments—minimally checking immigration status. Unsecured computers left logged on, passwords and codes for copying machines taped to inside desk drawers, loose documents on desks, notebooks beside experiments left running at night—all represent potential security risks.

Cyber-attacks reveal every industry's vulnerability

Until recently, an international competitor or a terrorist group wishing to obtain and capitalize on a pharma company's confidential technology would have had to recruit multiple scientists and manufacturing engineers, or insert operatives as employees capable of stealing lethal organisms or chemicals. Today, however, criminal, political, and terrorist groups might use teams of dedicated hackers to steal the same information an intruding terrorist masquerading as a scientist might try to obtain. And evidence suggests they are doing just that.

According to a 2011 report by the US financial news network Bloomberg, international hackers have already penetrated the networks of top

pharma companies (Pfizer and Abbott), at least one medical device company (Boston Scientific)—and even the US FDA's Parkland, Maryland computer bank. The hackers, likely Chinese from their IP addresses, appear to have broken into the computer

it function like several computers) housed the equivalent of 88 different computer servers. Cornish used his familiarity with Shionogi's network to identify each of these virtual hosts by name or by its corresponding Internet Protocol address.

The deleted servers housed most of Shionogi's American computer infrastructure, including the company's e-mail and Blackberry servers, its order tracking system, and its financial management software. The attack effectively

froze Shionogi's operations for a number of days, leaving company employees unable to ship product, cut checks, or communicate by e-mail.

Cornish was eventually traced to the IP address of a McDonald's restaurant in Georgia where he'd charged a meal with a credit card at the time the Shionogi systems had been hacked. He was sentenced to 41 months in prison, and required to pay \$812,567 in restitution.

The Shionogi experience demonstrates just a small fraction of the risk of improperly secured computer systems, and failure to consider the possibility of criminal or terrorist acts by former employees who leave with valued information. The risk of cyber-access for pharma goes far beyond vandalizing a company's systems—it potentially spans criminal interest in a company's secret manufacturing and security technology, as well as providing the gist for political attacks designed to embarrass or damage the pharmaceutical industry.

Suppose, for example, a former pharma company IT specialist sells his access information to criminals with economic or political clients:

» The access information could be sold to international customers interested in mining the company's R&D computers for unpatented technology or secret manufacturing

Only formal security SOPs as rigorous as those for quality assurance and GMP can reduce the risk of involvement in a potentially fatal “imagination failure.”

systems of the hotel Internet services provider iBahn, used by traveling executives around the world. In addition to being able to view both unencrypted and encrypted e-mails, security authorities believe the iBahn hackers may have inserted malware to the laptops of those executives, enabling them to capture passwords typed by the executives.

The Shionogi case: What happens when pharma fails to monitor ex-employees

Every landlord knows to change the locks after a tenant leaves—but at least one pharmaceutical company didn't similarly change the internal passwords after an IT worker left—and suffered the consequences. Jason Cornish, a former IT specialist of Shionogi, Inc., the United States subsidiary of that Japanese pharmaceutical company, resigned just ahead of a major cutback that made redundant a former supervisor and close friend. In revenge for his friend's termination, Cornish gained unauthorized access to Shionogi's computer network using a “back door” he'd installed before his resignation. Cornish then used the secretly installed software program to delete the contents of each of 15 “virtual hosts” on Shionogi's computer network.

These 15 virtual hosts (subdivisions on a computer designed to make

technology. It could steal the company's unpublished adverse reactions reports, tests using laboratory animals, or information on the status of contract negotiations.

- » The same information could be used to access a company's HR records, where terrorists could find employees with internationally vulnerable families—employees who could be blackmailed to steal biologicals or toxins with terror potential, or to reveal technology such as how to produce the three-micron particles needed to weaponize agents like anthrax.
- » Counterfeiters might value knowing the source and composition of proprietary coatings and packaging materials, so they can more easily produce fakes capable of escaping detection by the closest visual examination.
- » Criminals in the raw materials supply chain may wish to exploit knowledge of incoming assay tests so they can subvert those tests by substituting cheap adulterated additives. Baxter's Chinese suppliers of heparin precursor knew about Baxter's safety inspection tests, and substituted cheap oversulfated chondroitin for expensive heparin precursor.
- » Other criminals in the supply chain may wish to learn how to penetrate track-and-trace security—or even the schedule of truck shipments to distant warehouses or wholesalers.
- » The Japanese terror group Aum Shinrikyo, responsible for a 1995 sarin gas attack on the Tokyo subway system, tried to manufacture anthrax and botulinum toxin from common non-pathologic strains. They didn't order pathologic forms from lab supply houses because of traceability after an attack. Today, a terrorist group might use its digital expertise to exploit gaps in a pharmaceutical company's computerized purchase-authorization

process to generate orders for dangerous biologicals, and to intercept those orders in transit—thus obtaining vastly more potent organisms than the ones the Japanese cult tried to culture and scale up almost 20 years ago.

The cyber threat to pharma from terrorist groups is especially troubling in Japan, because the surviving members of Aum Shinrikyo—regrouped under an organization named with the Hebrew letter “Aleph”—has morphed into a software company specializing in security software. Before its front company names were penetrated, Aleph sold its software programs to at least 10 government agencies, including the Defense Ministry, and more than 80 major Japanese companies. Although the software was removed when its developers were identified, Japanese security officials worry that inadvertent collaboration with terrorist-background individuals might have given them valuable information on how major companies and the government protect their secrets.

Pharma as a political target

Politically-based cyber-attacks on pharma came to international attention on December 8, 2012, when the global hacker group Anonymous announced via YouTube that it intended to attack the global pharmaceutical industry, in a manifesto dubbed “Operation Bad Pharma.” The goals of Anonymous appear to harmonize with those of domestic groups pledged to violence against drugmakers, like the UK Animal Liberation Front. In addition to targeting pharma, Anonymous proclaimed it intended to target Israel after the November 2012 rocket attacks on Israeli territory from Gaza—a troubling connection between anti-pharma international hackers and Mid-East militants.

Conclusion: act preemptively to prevent

For managers dealing with day-to-day business challenges, the security issues and risks raised here may seem too remote to merit in-depth consideration and development of action plans. Not since the unsolved 1982 Tylenol poisonings has the US pharmaceutical industry been even considered as potential vector through which a terrorist group or lone wolf might inflict death or illness on the general population. Since that episode, the pharma, cosmetics and food industries have all taken steps to protect their products against field tampering.

However, the industry faces a changed world with different political threats, and new technologies by which terrorists might exploit security gaps. Whether manufacturing brand or generics, solid dosage forms or injectables, every pharmaceutical company should reevaluate its procedures to prevent the entry of criminals and others through their HR departments, supply chains, warehouses, transportation systems, purchasing departments and computer networks. Only formal security Standard Operating Procedures (SOPs) as rigorous as those for quality assurance and GMP, and which are routinely reconsidered and tested, can reduce the risk of involvement in a potentially fatal imagination failure. **PE**

Miriam Halperin Wernli, PhD, is Vice President, Deputy Head Global Clinical Development and Global Head Business & Science Affairs, at Actelion Pharmaceuticals in Allschwil, Switzerland. She can be reached at miriam.halperin_wernli@actelion.com. **Boaz Ganor**, PhD, is co-founder of the International Centre for the Study of Radicalization and Political Violence (ICSR), a partnership of the University of Pennsylvania; the Interdisciplinary Center, Israel; King's College, London; and the Regional Center on Conflict Prevention (RCCP), Jordan. He is also deputy dean of the Lauder School of Government at The Interdisciplinary Center as well as executive director of the International Institute for Counter Terrorism (ICT), an academic policy research institute dedicated to innovative public policy solutions to international terrorism. He can be reached at ganor@idc.ac.il. They are co-authors of “Dangerous Liaisons” on pharma terrorism risk for World Pharmaceutical Frontiers and speak on this topic at meetings and workshops for security personnel.