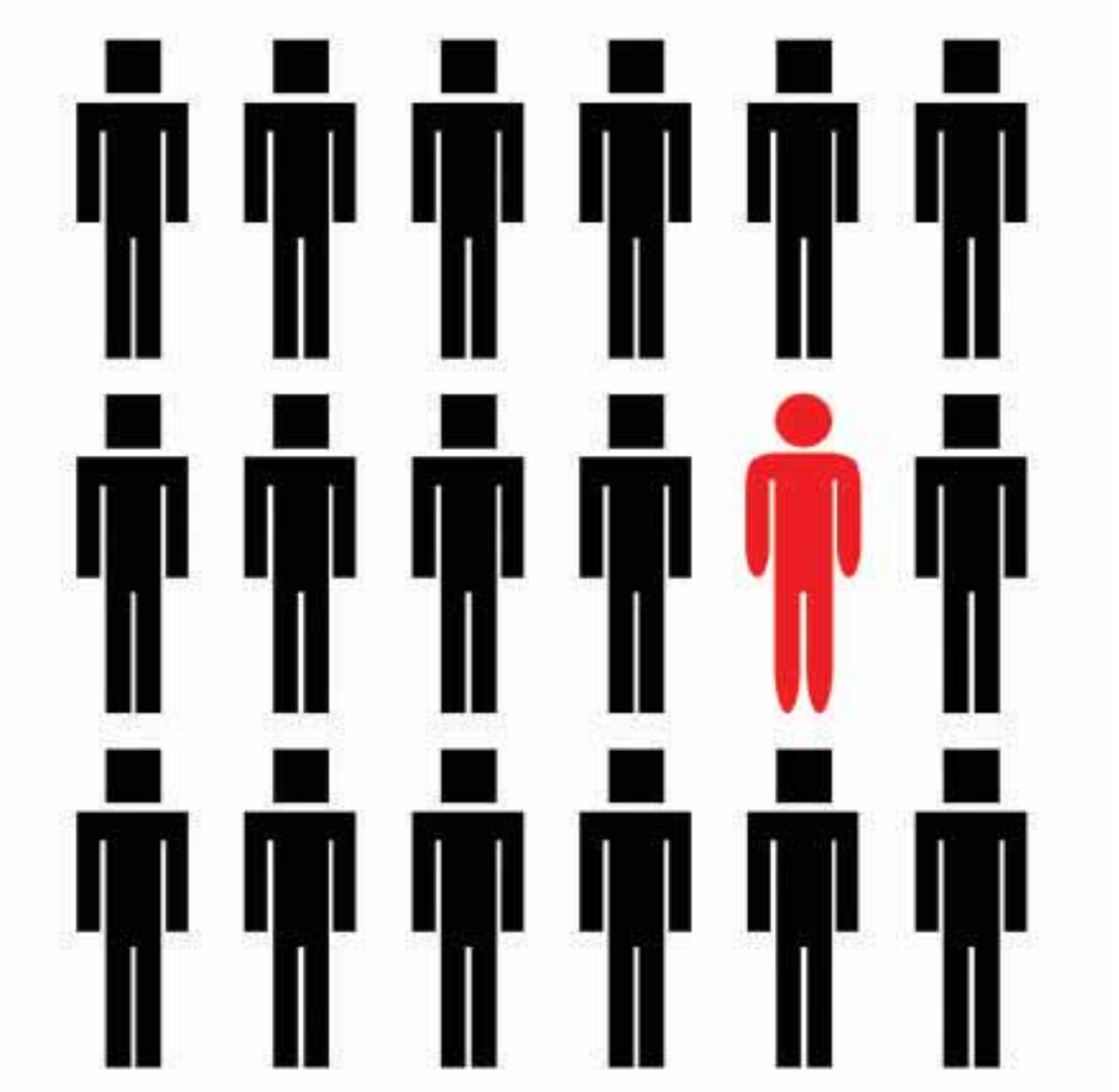

The Lone Wolf

As terrorist plots dominate the headlines, biopharma companies remain vulnerable to a wide range of intrusions motivated by criminal objectives. The industry cannot afford to neglect any data access gaps, or front door and inside job security deficiencies, to avoid compromising both employee and patient safety

Miri Halperin Wernli at Actelion Pharmaceuticals and Boaz Ganor at the International Institute for Counter-Terrorism

In 2001, shortly after the 9/11 attacks, the US experienced a series of mysterious anthrax cases, which were traced back to letters containing weaponised spores. Investigators concluded that the individual sending the letters was the same Department of Defense (DoD) scientist hired by the FBI to identify the spores' origin. It was also determined that the motive was not murder, but simply an attempt to communicate to superiors that the anthrax vaccine project should not have been cancelled. The DoD Human Resources (HR) Department and direct managers had written off warning signs of the sender's mental instability as "eccentricity".

While in the process of identifying the anthrax letter perpetrator, investigators first suspected another

bioweapons scientist, who was discovered to have a completely falsified CV and references. Both suspected and real originators of the attack presented credentials that – in the absence of careful reference checking and psychological testing – would have made them candidates for sensitive pharmaceutical/biopharmaceutical research positions. Had a terrorist group seeking technology or dangerous agents decided to recruit or blackmail a similarly credentialled individual, they might have successfully infiltrated a biopharma firm, if there was not rigorous HR screening in place.

More recently, Chinese and Russian hackers have relentlessly targeted the pharma industry, seeking to steal intellectual property (IP), as well as sensitive pricing and mergers and acquisitions (M&A) data. Some intrusions appear to have lasted many months before detection. Somewhat more disturbing is the discovery and conviction of 'lone wolf' employees stealing or destroying biopharma data – and, in at least one clear case, exacting revenge for management actions.

Means of Intrusion

These and other violations suggest that biopharma companies need to improve their security to better close four potential gaps:

- 'Front door' intrusion (entry through the hiring process) – usually by individuals inflating experience, but occasionally by criminals intent on fraud or theft
- 'Back door' intrusion (digital entry) – for theft of IP or financial data that could impact stock prices or health records, offering blackmail potential
- 'Inside jobs' by psychologically or personally vulnerable employees, or those with criminal intent
- 'Lone wolves' who, under the stress of family or financial pressures, mental disorders or politics, act in ways that can endanger other employees, management, customers or the general public

"More recently, Chinese and Russian hackers have relentlessly targeted the pharma industry, seeking to steal intellectual property, as well as sensitive pricing and mergers and acquisitions data"

Front Door Approach

While it is theoretically possible for a terrorist group like Al Qaeda or Islamic State (IS) to recruit a scientist and attempt to place him into a targeted company through its hiring process, far more likely intruders to introduce risk into a biopharma company are prospective employees who have falsified some, or all, of their CV.

Fake CVs

A poll of employers by CareerBuilder, the biggest US online employment website, revealed that 29% have discovered falsified references on a candidate's resume (1). Meanwhile, according to a survey conducted by AuthBridge, the highest rate of CV discrepancy – 37.31% – was found in pharma/biotech/clinical research companies, because "unlike the IT industry, they weren't early adopters of background verification" (2). Most egregious are instances where candidates pay for referrals from fake companies that will, during reference checking, verify the CV claims.

Aside from their likely incompetence in key areas, such individuals can subject the firm to financial losses and drive away competent prospects. The British biotech firm QIAGEN hired an HR manager based on his claim of a Master's degree in Human Resource Management from Manchester Metropolitan University (3). His fabrication was not discovered until after he had collected almost £40,000 for unapproved and unattended training courses, £5,000 for travel, and £500 for a hotel Christmas party.

While he was convicted of fraud and is serving a three-year prison sentence, his employer is left with unanswered questions: during his time in that role, were qualified candidates turned away? And, of significant concern, were unqualified ones hired?

Biotech is not unique in its 'front door' failures: David Tovar, Walmart's Vice President for Corporate Communications and an eight-year employee, was forced to resign when the company discovered he had lied about having graduated from the University of Delaware, US (4). While most employees are fired or resign when their employers realise they have falsified part, or all, of their CVs, some may be vulnerable to blackmail to silence an individual or group threatening exposure.

Checking All Candidates

Pre-employment screening for biopharma should not be limited to just potential laboratory and C-suite hires. The *Chicago Tribune* reported on a suburban pharma firm that discovered $500,000 worth of computers and parts had gone missing. A subsequent investigation revealed that gang members had been unwittingly hired for positions in shipping and receiving, and the stolen computers and parts were being purchased and resold by a collaborator at a local storefront. Further enquiry determined that the gang members were also selling drugs to fellow employees. In another instance, a contract security guard at a chemicals company was bribed to steal a highly sensitive scale and smuggle it out to a gang involved in drug trafficking (5).

Back Door Strategies

Today, the greatest threat to a company, its customers and employees is likely to stem from demonstrated 'back door' vulnerability of its computer systems – mostly from international hackers, but also from current and former employees with IT knowledge and a grudge, or any contractor with access to company data.

Ex-Employees

A former IT staffer at the US facility of the Japanese company Shionogi executed one of the most shocking back door intrusions in pharma history. According to a statement by US Attorney Paul Fishman, James Cornish had resigned from Shionogi in September 2010, after the company announced job cuts that were due to affect a close friend of his who was also a former supervisor (6).

To carry out the attack, Cornish accessed the Shionogi computer system from a laptop, using the Wi-Fi network of a local McDonald's in his hometown in Georgia. Once logged on, he activated software he had secretly installed weeks earlier, deleting the contents of 15 'virtual hosts' that housed the equivalent of 88 computer servers – erasing most of Shionogi's American computer infrastructure. The attack effectively froze Shionogi's operations for days, leaving employees unable to ship product, cut cheques or communicate by email, according to a statement issued at the sentencing. Cornish was given 41 months in prison and ordered to pay $812,567 in restitution to Shionogi.

Hacktivists

While the Obama administration and FBI believe North Korea was responsible for the recent Sony hack, security firm Norse analysed a stolen Sony Excel file of terminated employees posted on the 'dark web'. The company claims it found evidence that the hack may have been perpetrated by six individuals, including two based in the US, one in Canada, one in Singapore and one in Thailand (7).

Norse told a security industry news website that among the six was a former Sony Pictures IT veteran who had worked for ten years at the company, but had been laid off in a recent restructuring. Their researchers followed the individual online, observing angry posts she had made on social media about Sony and the layoffs. Through access to Internet Relay Chat forums and other sites, they captured her communications with others affiliated with underground hacking and 'hacktivist' groups in Europe and Asia.

The security company also claims that malware completely in English, and not in Korean, existed on the Sony servers as early as July 2014. They suggested that Sony credentials, server addresses and digital certificates were built into the malware – data virtually impossible for hackers to get hold of unless they were an insider, or had been working with one (8).

Furthermore, the criminals who had hacked the servers threatened the company's customers, employees and employee's families. Someone claiming to represent the hacker group Guardians of Peace sent emails to Sony Pictures employees in which they promised to bring about the collapse of the firm. The message asked that employees join the hackers in denouncing Sony Pictures. "If you don't," the message said, "not only you but your family will be in danger" (9).

The implications of hackers getting hold of an entertainment company's employee and customer data are serious, but a similarly successful hack of a biopharma company's employee, customer, investigator and regulatory databases could be vastly more damaging and dangerous. Confidential exchanges between regulators and investigators could be disclosed, as well as home addresses of lab researchers revealed to animal rights picketers, for example.

Drug Heists

The largest drug heist in US pharma history occurred when thieves cut into the roof of an Eli Lilly warehouse in Enfield, Connecticut, and loaded $80 million worth of prescription drugs into a rented trailer truck. Eli Lilly's insurer, National Union Fire Insurance Company, claimed in a civil suit that the thieves were guided by a vulnerability assessment conducted for the company by security firm ADT.

The ADT assessment showed the location of 13 cameras inside the warehouse and the grid coordinates on a floor plan for every motion detector, infrared beam, door contact and control panel within

"The implications of hackers getting hold of an entertainment company's employee and customer data are serious, but a similarly successful hack of a biopharma company's employee, customer, investigator and regulatory databases could be vastly more damaging and dangerous"

the security system. The thieves loaded approximately 49 pallets of Zyprexa®, Cymbalta®, Prozac® and Gemzar® into a trailer parked in the only one of seven loading docks not visible to security cameras. One of the thieves, with an extensive criminal record, left identifiable DNA on a water bottle at the scene, and was apprehended selling the stolen drugs from a rented warehouse (10,11). The exact method by which the ADT information was passed to the thieves is still unknown; however, one of them was a self-employed alarm installer.

In another example, hackers with Wall Street expertise have been stealing M&A information from more than 80 companies for over a year, according to security firm FireEye Inc. The company claims a group dubbed 'FIN4' has been tricking executives, lawyers and consultants into providing access to confidential data and communications, and is suspected to be using the information for insider trading. Most of the cases detected have involved healthcare or pharma companies whose stock prices depend on news of mergers, clinical trial results and regulatory decisions (12).

Vendor Targets

Biopharma companies routinely entrust sensitive information to vendors such as preclinical labs, contract sales organisations and investor relations firms. On 17 October 2007, IMS Health had planned to announce negative earnings via an investor relations service after the market closed. Earlier that day, individual trader Oleksandr Dorozhko secretly hacked into the secure computer network of Thompson Financial – which hosted the IMS Health investor relations website – and stole IMS Health's earnings information (13).

Within minutes of this hack, and just before the scheduled earnings release, Dorozhko purchased 630 put options on IMS shares. After the market closed, the company reported third quarter earnings that were significantly below analysts' consensus estimates and the previous year's earnings for the same period. The next day, its stock price fell 28% to an all-time low, and Dorozhko sold all of his put options, realising profits of approximately $287,346.

The United States District Court for the Southern District of New York ordered Dorozhko to pay approximately $580,000 in disgorgement, prejudgment interest and a civil penalty.

Inside Jobs

Theft of information and electronic data at global companies has overtaken physical theft for the first time, according to the latest edition of the Kroll Annual Global Fraud Report – an international study that surveyed more than 800 senior executives worldwide. The results show that the amount lost to fraud rose from $1.4 to $1.7 million per billion dollars of sales in the past 12 months – an increase of more than 20% (14).

According to Robert Brenner, Vice President of Kroll's Americas region, theft of confidential information is on the rise because data is increasingly portable. Perpetrators – often departing or disgruntled employees – can steal or destroy data with ease in the absence of sufficient controls.

According to the report, junior employees and senior management were the most likely perpetrators at 22% each, followed by agents or other intermediaries at 11%. The proportion of fraud carried out by these employees ranged from 50-60% in North America, Europe and Asia-Pacific, to 71% in the Middle East and Africa. The figure dropped to 42% in Latin America, where customers are the primary fraudsters.

IP Theft

One of the industry's most notorious inside job thefts of IP occurred in the biologicals development facilities at Bristol-Myers Squibb (BMS), New York. Shalin Jhaveri was employed in a management training programme at the facility, and used a company-issued laptop to steal manufacturing and testing data for an anti-human CD137 monoclonal antibody, which was under development to treat malignant melanoma. His actions came to the attention of the BMS Information Security Division, which detected that Jhaveri had accessed the drug development files. Computer forensic analysts recruited by BMS made a remote image of the work laptop, and determined he had downloaded 45 gigabytes of data into the 'My Documents' folder, transferred the files to an external hard drive, and then deleted the folder (15).

The BMS review of the laptop image revealed Jhaveri planned to start a biopharma company in India. He communicated to a prospective investor using a specially created email account and password he set up expressly for that purpose. The forensic software – including keystroke monitoring – determined that he had received an email from an individual in India with an attachment concerning a business plan model for what appeared to be a cell culture products company. Following a meeting with an FBI agent posing as a prospective investor, Jhaveri was confronted and admitted his crime. He was fined $5,000 and deported (15).

Lone Wolf Threat

The idea of a terrorist seeking to gain employment in a Western pharma company – with intent to steal technology of terror value – would appear remote. However, the ability of IS to recruit technologically skilled experts in many fields suggests this possibility deserves at least a brief mention in a human element risk discussion.

Sarah Teich from the International Institute for Counter-Terrorism cites the work of several researchers who conclude lone wolves create their own ideologies, combining personal frustrations and aversions with broader political, social or religious aims. In the process, many draw on internet-enabled 'communities of belief' and 'ideologies of validation', generated and transmitted by extremist movements – and not necessarily religious ones (for example, right-wing, anti-abortion and anti-immigrant groups). Discontent about workplace respect, financial stresses, divorce or other family problems –

or a potentially toxic combination of all – can increase susceptibility to groups like IS (16).

What sharply differentiates IS from prior movements is its demonstrated ability to incite homegrown, self-radicalised Western individuals to commit terror in their country of residence. Although remote, management must be sensitive to the possibility of a vulnerable, radicalised employee.

Despite the extremely low likelihood of a self-radicalised employee perpetrating an attack, managers need to be aware if an employee demonstrates personality changes or unprecedented aggression. The highest likelihood is that personal life stress can explain mood changes – and demonstrated management understanding to the employee can be reassuring to all. But such discussions could surface deeper issues that may require HR evaluation – especially if the conversation turns from personal to clearly antisocial expression.

Teich notes that lone wolves tend to be much less secretive earlier than their attacks may suggest. Without being unnecessarily intrusive, management needs to be sympathetic to employee reaction to workplace changes that suggest personal issues may be troubling them – especially if others report concerns. Lone wolves frequently vent their feelings in social media prior to acting. Commonly, after a lone wolf incident, family, friends and co-workers express prior awareness of the perpetrator's discontent, but usually underappreciate it.

Mind The Gaps

Biopharma companies are vulnerable to a broad range of intrusions, motivated by criminal objectives or intimidation. Wise managers appreciate that security professionals can contribute to closing back door data-access gaps, and can detect potential front door and inside job security deficiencies, but firms cannot afford a failure of imagination in closing off even the most remote intrusion possibilities.

References

1. Nearly three-in-ten employers have caught a fake reference on a job application, Career Builders press release, 28 November 2012. Visit: www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=11/28/2012&id=pr727&ed=12/31/2013
2. Madhusodan MK and Phadnis S, Fake companies help fluff CVs for a fee, *The Times of India*, 29 September 2013
3. Thompson D, Man lied about degree to get job, then conned employer out of £50k in expenses, *Manchester Evening News*, 11 June 2014
4. Hamm M, Spot the fake CV, *In the Black*, 1 December 2014
5. Buck G, Gangs find crime pays better when on the job, *Chicago Tribune*, 28 September 1997
6. Voreacos D, Ex-Shionogi worker gets 41 months for computer hacking, *Bloomberg Business*, 9 December 2011
7. Robers PF, New clues in Sony hack point to insiders, away from DPRK, *The Security Ledger*, 28 December 2014
8. Liebelson D, Ex-Sony employees echo cybersecurity company's suspicion that hack was an inside job, *Huffington Post*, 7 January 2015
9. Huddleston T, Sony Pictures employees get threatening email from alleged hacker, *Fortune Magazine*, 5 December 2014
10. Ofgang E, New guilty pleas in Connecticut's biggest heist at Eli Lilly warehouse, *Connecticut Magazine*, 25 November 2014
11. Fifth defendant in Eli Lilly warehouse theft case pleads guilty, US Department of Justice, 25 November 2014. Visit: www.fbi.gov/newhaven/press-releases/2014/fifth-defendant-in-eli-lilly-warehouse-theft-case-pleads-guilty
12. Levin A and Riley M, Hackers with Wall Street savvy stealing M&A data: FireEye, *Bloomberg Business*, 1 December 2014
13. SEC obtains summary judgment against computer hacker for insider trading, US Securities and Exchange Commission, 29 March 2010
14. Information theft at companies surpasses all other forms of fraud for first time, *Security Week*, 18 October 2010
15. Former employee of Bristol-Myers pleads guilty to theft of trade secrets, FBI Albany Division, 5 November 2010
16. Teich S, Trends and developments in lone wolf terrorism in the Western World, International Institute for Counter-Terrorism. Visit: www.ctcitraining.org/docs/LoneWolf_SarahTeich2013.pdf

About the authors

Miri Halperin Wernli currently holds the position of Vice President, Deputy Head Global Clinical Development, and Head of Global Business and Science Affairs at Actelion Pharmaceuticals, Switzerland. She completed her PhD in Genetics and Experimental Psychology at Geneva University, complementing her studies with clinical training in Child and Adult Psychology in Toronto, Canada, and an Executive Business MBA from Stanford Business School, US. Miri has held a range of managerial positions within global pharma companies, including Merck, Sharp & Dohme and Roche Pharmaceuticals.
Email: miriam.halperin_wernli@actelion.com

Professor Boaz Ganor is the Dean of the Lauder School of Government at the Interdisciplinary Centre, Israel, and Executive Director of the International Institute for Counter-Terrorism – an academic policy research institute dedicated to developing innovative public policy solutions to international terrorism. He is also the co-founder of the International Centre of Radicalization and Political Violence. Boaz holds a PhD and BA in Political Science from the Hebrew University, and a Master's degree from Tel Aviv University, Israel.
Email: ganor@idc.ac.il