THE CONVERSATION
Academic rigor, journalistic flair

# How governments and companies can prevent the next insider attack

February 20, 2017 8.19pm EST

An insider can bypass many layers of security. Los Alamos National Laboratory

## Authors

**Matthew Bunn**
Professor of Practice, John F. Kennedy School of Government, Harvard University

**Scott D. Sagan**
Professor of Political Science, Stanford University

Now that they are in office, President Donald Trump and his team must protect the nation from many threats – including from insiders. Insider threats could take many forms, such as the next Edward Snowden, who leaked hundreds of thousands of secret documents to the press, or the next Nidal Hasan, the Fort Hood mass killer.

Indeed, in today's high-tech and hyperconnected world, threats from insiders go far beyond leakers and lone-wolf shooters. A single insider might be able to help adversaries steal nuclear material that terrorists could use to make a crude nuclear bomb, install malware that could compromise millions of accounts or sabotage a toxic chemical facility to cause thousands of deaths. How can we better protect against the enemy within, no matter what it is that needs to be protected?

President Obama became so alarmed at the government's weak protections against insiders that he created a "National Insider Threat Policy." It required each federal agency to put in place a set of basic

safeguards against internal betrayals, such as software to detect mass downloading of secret documents and systems to encourage reporting of worrying behavior.

But President Trump will find there is a great deal still to be done. This is in part because the insider problem is so challenging. Insiders are known and trusted by other employees (and have to be, if the organization is to function well); they may have detailed knowledge of the security system and its weaknesses; and they can take months or even years to plan their activities.

We co-organized a research project to investigate this challenge and suggest potential solutions, which led to our new book, "Insider Threats." The book was prepared as part of the Global Nuclear Futures initiative at the American Academy of Arts and Sciences. The volume analyzes a range of situations as diverse as Afghan Army soldiers attacking their U.S. trainers and the anthrax attacks in the United States in 2001 – which were probably perpetrated by Bruce Ivins, a disturbed scientist from the U.S. Army's biological defense lab. The cases reveal a series of hard-learned lessons that can help organizations protect against threats from insiders.

### 'Not in my organization'

First, a remarkable number of people wrongly assume their workplace couldn't possibly be threatened by insiders. That is a bias we dub "NIMO," for "not in my organization." That overconfidence can have fatal consequences.

In 1984, for example, Indian Prime Minister Indira Gandhi was killed by two of her own Sikh bodyguards, one of them a trusted favorite. Her security chief had even warned her to remove the Sikhs from her guard, citing Sikh anger about an Indian military attack on Sikhism's holiest site, the Golden Temple.

Killed by insiders: Indira Gandhi. Dutch National Archives, CC BY-SA

### Missing the red flags

One of the most striking elements of the cases in our study is how organizations ignore even the most obvious and alarming red flags. U.S. Army biodefense researcher Bruce Ivins, for example, complained about his increasingly dangerous paranoia in an email to a colleague. Ivins even speculated about being mentioned in newspaper reports with the headline: "Paranoid man works with deadly anthrax."

No one reported, or acted on, that or any of his many other signals that something was amiss. Instead, his coworkers wrote them off as harmless eccentricity. Even when an employee told his boss that she feared he would attack her, no action was taken.

Companies and government agencies must provide strong incentives for their employees to report worrying behavior – including clear and well-enforced reporting rules, and recognition for those who do the right thing. Those efforts should make clear that in some cases, the result of reporting will be that a troubled colleague gets much-needed

help.

### Disgruntlement dangers

Employees who are upset are far more common than mentally disturbed ones, and therefore more likely to pose an insider threat. One study of insider cyber-sabotage found that 92 percent of the cases examined occurred "following a negative work-related event such as termination, dispute with a current or former employer, demotion, or transfer."

More than half of the insiders in these cases were already seen as disgruntled before the incident occurred. Fortunately, simple steps can combat employee dissatisfaction. These include providing effective processes for making and resolving complaints, complimenting and rewarding employees for good work and reining in bullying bosses.

### Multiple layers of defense

Organizations often make the mistake of thinking a single element of defense – such as background checks – is enough to protect them from insiders. But defenses are often less effective than they seem. Years ago, for example, Roger Johnston and his colleagues in the Vulnerability Assessment Team at Los Alamos National Laboratory tested over 100 types of widely used tamper-indicating seals. They found that all of them could be defeated with equipment from any hardware store, with average defeat times of less than five minutes.

Hence, organizations need a comprehensive approach to protecting against insiders, from ensuring that no one can access the protected items without being monitored to building a vigilant, questioning culture. Nuclear facilities, for example, should keep material that could be used in a nuclear bomb in a locked vault to which few have access, constantly monitor the vault, ensure that no one is ever in the vault alone and, where practical, keep the material in forms too big and heavy for one person to carry and hide.

Monitoring people, information and physical spaces can be critical. After an insider destroyed a nuclear reactor's turbine in Belgium in 2014, for example, the country established new rules ensuring no one could ever be alone and unwatched in key reactor areas.

A turbine at this Belgian nuclear plant was destroyed by insider sabotage in 2014. Torsade de Pointes

Testing and constantly looking for vulnerabilities are also key. Johnston's effort is only one example of an essential approach: assigning intelligent teams to look for ways to defeat security systems, identifying weaknesses and helping to fix them.

Building a strong security culture in the organization – in which all employees take security seriously and are constantly on the lookout for vulnerabilities to be addressed or concerning behavior the organization should know about – is fundamental. The Fort Hood massacre can be blamed, in part, on a breakdown of security culture. Despite clear danger signs in erratic behavior and radical statements, none of Nidal Hasan's commanders wanted to cope with the hassle of disciplining him.

Fixing these systemic problems takes focused leadership from the top of the organization, incentives for strong security performance and a broad understanding of both the threat and the relevance of security measures to deal with it throughout the organization. Capable leadership will make organizations more successful and more secure.

In our high-tech society, the insider threat is ever-present. High-security organizations, governments and companies alike need to take action to counter the organizational and cognitive biases that often blind us to the insider danger – or future blunders will condemn us to more disasters.

**Security** **Anthrax** **Trust** **Nuclear policy**