All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The insider turned bad

Insiders – those with legitimate access and authority – are often cited as the most damaging information-related threat. But how do insiders turn bad, and what can be done about them?

Turning

A fundamental to understanding insiders who turn, as opposed to those who become insiders intending to be malicious all along[1] or those coerced into discreet acts of disloyalty,[2] is that turning is a behavioral change that happens for a reason. Well intentioned loyal individuals who do their work day-to-day in support of those they work for and with, don't become disloyal instantaneously, and don't all of the sudden show up one day completely changed. At least that's not what studies of the field have shown.[3,4,5,6] Rather, they start down the path to turning in a slow process that is enhanced by the feedback they get from their environment, elements of their personality, and their real or perceived situation.[7] The process of turning leads people to levels of disgruntlement and, over time, they start to push further and further into the realm of action that is adverse to their position as an insider.

Recognized behavioral traits and responses that fail to address them

There are usually signs of turning and, in many cases, they are observed by others in the workplace, including management. Typical patterns of interaction within the workplace have been asserted to involve management recognizing a problem, but dealing with it ineffectively. The most problematic and harmful of these situations involves management believing that the insider who is behaving badly should be punished but retained in the position of responsibility.

- In some cases, the claim is made that they are too valuable to get rid of, and of course this should never be the case in any but the smallest of businesses.
- In other cases, they are so high in the management chain that the only ones who can act are top-level managers who are reticent to believe that those they are working with would turn on them.
- The nature of workplaces often prevents those empowered to act from taking effective action. They merely force the insider to act more surreptitiously and turn further.

[1] Sometimes called “sleepers” or “plants”.

[2] For example individuals whose family members are kidnapped and who are then coerced into bad acts.

[3] M Keeney, E. Kowalski, D. Cappelli, A. Moore, T, Shimeall, S. Rodgers, “Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors”, Jan 2005.

[4] E. Shaw, K. Ruby, and J. Post, “The Insider Threat to Information Systems - The Psychology of the Dangerous Insider ”, Security Awareness Bulletin, No. 2-98, 1998.

[5] E. Shaw, K. Ruby, and J. Post, “Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, Recommendations”, Aug 31, 1999. ASD-C3I – OIO - Contract # 98-G-7900, Task Letter Number 001:Insider Threat Profile.

[6] E. Shaw, K. Ruby, and J. Post, “Insider Threats to Critical Information Systems: Characteristics of the Vulnerable Critical Information Technology Insider (CITI) Contract Nr. N39988-97C-7850, Sep 25, 1998.

[7] CERT insider threat center [http://www.cert.org/insider_threat/] has several papers in this area.

What can we do about them

Here lies the rub. Nobody wants to terminate workers who haven't yet gone over some threshold of behavior that is definitively unacceptable, and even things that are definitive must be compared to other behaviors let slide before. Otherwise, discrimination, wrongful termination, and other similar issues may come up. And yet, inaction will not stop turning behaviors, and attempts at retribution or punishments that don't sever the relationship have a tendency to amplify rather than subdue the turning behavior. At least that's what the studies tend to show. So what to do?

Here are some alternatives that might work for you. When you identify an insider who seems to be turning (however you do that), try this:

- **Risk mitigation:** Move the individual to a position better aligned with their interests and abilities and less risky to the organization. In this way, their job will get better and risks will be reduced. Perhaps if they prove themselves useful there, they can be moved into a different position after that and eventually reach the same level of trust they previously had. Along the way, make sure you use proper process to assure that their access is no longer available to the previous job functions.
- **Risk avoidance:** Identify potential turning behaviors earlier through a systematic program, and mitigate the circumstances that are causing them. Must turning behaviors are associated with emotional changes in a person's life, stress caused by relationships, money, personal loss, life cycle issues, and other similar sorts of things. To the extent that the behaviors or conditions can be detected earlier, they may be better handled through counseling, a more understanding workplace, time off, reduced stress in responsibilities, and so forth.
- **Risk control and transfer:** Many insurance policies provide protection against insider frauds, key persons, and similar hazards. Of course less expensive policies mandate better internal controls, such as strong separation of duties, risk aggregation limits, multiple signatures required for financial transactions above thresholds, a strong approval chain process, and so forth. Risk controls should deal with insiders as well as outsiders, and insurance may be used to mitigate against catastrophic insider failures to a limited extent.
- **Risk acceptance:** While some level of insider risk must always be accepted, it is key to understand just how much risk is being placed where, and to limit it as a matter of policy and operations. Risk acceptance should normally be understood and, to the extent risk-related issues are otherwise documented, it should be made explicit in policy and procedure.

Conclusions:

Many insiders turning are already detected by outward signs. Cases like the Fort Hood and Virginia Tech shootings could not have had clearer indications in advance. The WikiLeaks case and other cases we have examined show obvious workplace observables. In case after case, we find that some in management knew, but nobody acted adequately to mitigate the harm. At the end of the day, no matter what we do to detect insiders turning, unless and until we are willing to act on the information we have, these sorts of problems will continue.