Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Social tension and separation of duties:

People issues have always been key to information protection, and yet they are under-served because of the high level of technology involved in the emerging information age. This month, the focus is on people issues, and in particular the intentional introduction of social tension into the workplace in order to have effective separation of duties.

Most executives that I know are generally opposed to having an organization that is in eternal internal conflict. As a result, it may be hard to sell them on the notion that we need to foster internal eternal conflict between certain individuals and groups as part of the strategic approach to having effective information protection. Why can't we all just get along? We have enough of a problem fighting as a team against our competitors, market forces, and the business environment - why would we actually want internal conflict? Perhaps it is a matter of wording. Let's call it healthy competition instead of conflict, and perhaps it will be more palatable.

Competition fosters innovation and increased effort, more cohesion within groups, and a social environment of making more rapid progress. It is highly motivating if properly done. So what are the competing interests I speak of? They are the issues associated with separation of duties.

Separation of duties is fundamental to protection in that it mitigates against a single individual abusing their authorization. If the same person who handles payments also handles purchases, they can create a purchase and pay for it, thus doing everything involved in moving money out of the enterprise. By properly using separation of duties, it takes two people to get this done, and they have to collude in order to move money out. They normally do collude - on legitimate purchases - and independently of each other through the purchasing and payments process. Of course that's where the problems really begin.

The problems with separation of duties as done today comes in a variety of different areas. For example, the IT system that handles purchases may be a single computer with one individual who is able to do anything - a superuser who can directly access the databases, for example. Separation of duties must be applied at all levels and to all interdependent functions to have adequate assurances for high consequences. But this and related issues is not what this article is about. I just mentioned it to let you know that it's more complicated the deeper you dig into it.

The problem I wanted to discuss, however, was a different one. How do we keep the people involved in the separated duties from colluding and breaking the system that way. I know the old saw about being paranoid, and the notion that two supposedly independent people could or would get together to perpetrate a fraud could never happen, and the one about we can't work with people we don't trust. But that changes nothing. I have personally seen a situation where the head of HR was (literally) in bed with the head of IT. Collusion happens.

So how do we reduce the risk of collusion? We could make it so the people securing perimeters don't know the people doing independent perimeter verification, and this can work well. Except that it makes it a lot harder to coordinate efforts if there is no communications. We can use independent testers and audits to try to verify things, but that just means that they fixed the hole when the auditors were looking. We can do double blind super secret audits - or find a better name for them to make them more appealing. All of these things work to some extent. But here's another idea.

Suppose we set up intentional social tension between groups whose duties are separated. In this scheme, we might, for example, make it a competition with rewards and punishment. The perimeter verification folks and the perimeter operators compete over a fixed total bonus pool. There is scoring so that successful penetrations by the testing team (following the rules of course) wins them bonuses as a team, while the failure to penetrate wins bonuses for the folks operating the perimeters. Each is highly motivated to do their jobs well, and depending on the magnitude of rewards, may perform at enterprise desired levels, or in excess of them.

But is money enough to dissuade collusion between people who stand to gain far more than their bonuses by working together? I think not. I have seen cases where two individuals who worked together every day could collude to steal more than 100 million dollars. How much of a bonus is likely to be needed to deter that kind of theft? Is money really the motivator, or is there something else that might work better? How about group cohesion?

Small unit cohesion in the military results in individuals giving up their lives to save the lives of their fellow soldiers. Group cohesion keeps gangs together against other gangs. Charismatic leaders generate the kind of loyalty that produces mass suicide within those groups on occasion. Party loyalty generates dogmatic responses to questions and rapid shifts in expressed views, even when they are completely inconsistent with expressed views only days before. Religious groups, fraternities, terrorist groups, and secret societies have all produced extremes in loyalty through social pressure and a wide range of other similar tactics. And even team sports generate love for team mates and hatred for rivals.

So in the quest for ways to reduce the risks of collusion, isn't it a possibility to use some of the same influence tactics and strategies to generate greater loyalties in the separation of duties? I think it is feasible to do so, but not to the point of extremes. For large enterprises, it is entirely feasible to have payables and purchasing groups located in separate cities and to foster group cohesion and internal rewards while punishing collusion or even communications across the groups. Team sports, competitive business-relevant training games and scoring, group charitable activities with competitive donation levels and rewards dinners, and even the creation of propaganda, can all be used to reduce the potential for collusion while generating positive outcomes for the individuals and the enterprise. For smaller companies, lighter weight versions of the same activities can be used, but they are likely to be less effective.

Group cohesion and social tension are techniques that can be meaningfully applied to security, particularly in the area of separation of duties. Whether they will is another matter. Many enterprises may have misgivings about the use of such tactics when explained in this way, but they likely already use many of the same tactics with regard to competitors, in sales and marketing, and in the development of strategic plans. If the stakes are high enough...