EMPLOYEES BEHAVING BADLY?

DEBI ASHENDEN

Most of the literature on insider threat focuses on either the 'malicious' insider or the 'accidental' insider. But what about those individuals who know what they should be doing but choose to deliberately breach security because they think it's in the interests of their organisation?

I've started calling these 'everyday insider threats'. Industry reports tell us that employees often admit to breaching security because it 'gets in the way.' A significant proportion of these individuals also believe that they won't get caught. These are deliberate but not necessarily malicious acts. They are often small individual actions that unfortunately have the potential for significant organisational impact.

IRRATIONAL BEHAVIOUR

Traditionally, security research has taken a rational approach to understanding the insider threat. This approach features in the Simple Model of Rational Crime and also in broader theories such as the Theory of Planned Behaviour and the Theory of Reasoned Action. The assumption of these theories is that employees consider the potential costs (will I get caught?) against the potential benefits (what will I gain?) before misbehaving. Such a perspective has merits. We know from research that, under some circumstances, offering financial (or other) incentives along with priming on possible consequences, supplying extensive feedback, and giving training, can deter people from breaching security.

However, it doesn't work reliably. What seems rational to the expert manipulating the cost/benefit exchange isn't always rational to the individual carrying out the behaviour. There are other factors at play, and thresholds to costs and benefits vary across individuals. The rational approach may also be used to offload responsibility. The security practitioner argues, 'but we told them why they shouldn't do it,' and the employee responds, 'but I couldn't do it any other way'. Finally, what works in a lab when such a cost/benefit exchange is negotiated doesn't always work in the real world. Things are more complex.

It seems that good people can do bad things and, unfortunately, what looks like rational behaviour to one person (the security practitioner) does not to someone else (the employee). So what's really going on here and is there something we can do about it?

There is a wealth of research on the concepts of workplace deviance, counterproductive workplace behaviour and organisational citizenship behaviour. Workplace deviance and counterproductive workplace behaviour are intentional behaviours that cause harm to the organisation. Organisational citizenship behaviour is voluntary behaviour that benefits the organisation. These three kinds of behaviour are linked but the first two are not opposites of the third. An employee can do both, or do one when they think that they are doing the other.

LOAFERS, FREE-RIDERS AND SUCKERS

There are at least three possible explanations coming out of research that might explain why employees do what they do. The first possibility is 'social loafing'. Individuals hide in the crowd and think that nobody will notice their limited contribution, or that they're breaching security. The second possibility is the 'free rider effect'. Individuals perceive that their misbehaviour doesn't matter because sufficient people are doing the right thing. In security terms this might be when there is a reliance on the technology or business processes to deliver security rather than the actions of an individual employee. The third possibility is that employees don't want to be seen as 'suckers'. They see others breaching security and conclude that if others aren't complying then they don't need to either.

> **Good people can do bad things and unfortunately what looks like rational behaviour to one person (the security practitioner) doesn't to someone else (the employee).**

Fortunately, there are interventions that can help organisations counter all three of these assumptions. Ensuring employees know that their actions can be identified, giving them feedback on a regular basis, and presenting compelling evidence that their contributions are important, have each been shown to help. As has enabling employees to compare their behaviour with those of others, since it decreases social loafing. Finally, encouraging group cohesiveness can also help to ensure employees are given opportunities to help each other, though the effects of this has yet to be explored in a security context.

SPENDING BROWNIE POINTS

So that's the problem of the 'everyday insider threat' solved then isn't it? Unfortunately, it's not that straightforward. Individuals can be tricky and again, while these interventions will help in certain circumstances, there are instances where research has shown they won't work. For instance, it seems that good deeds by an employee can mean that she or he feels entitled to act badly in the future. The greater the reward for compliance the more 'naughty' it can feel to not comply. Moreover, organisations like their employees to be creative and innovative but these traits are often positively associated with misbehaving. Thresholds for how employees can misbehave and yet still feel good about themselves vary a lot.

It seems, then, that there's good news and bad news. While the interventions outlined above are a good starting point, they can't be relied upon to work every time. These interventions also give us an interesting research proposition – how much will people 'cheat' at security and under what conditions? How can we better understand the trade-offs that employees make and what is really happening underneath the mandated processes and policies? Can we improve security by, rather counter-intuitively, making people jointly responsible for compliance rather than individually responsible? These are the questions that the Protective Security and Risk programme of CREST are addressing.

To find out more about this research visit the CREST website (www.crestresearch.ac.uk).