The Insider Threat: a Problem wrapped in Perplexity.

Karen Renaud (University of Strathclyde – karen.renaud@strath.ac.uk)

The insider threat is a real problem for modern organisations. The human is undeniably a lot harder to secure than technical parts of the socio-technical system. The traditional approach is to formulate policies, disseminate them during awareness drives, and mandating compliance. When someone makes a mistake like clicking on a phishing message, they are sent for retraining. This approach relies on two assumptions: (1) knowing=doing, and (2) compliance will reduce the insider threat.

These assumptions are flawed. 'Ought' is not the same as 'can'. There are many reasons that prevent employees from acting on their knowledge: e.g., their mental state or impaired capabilities. Morever, compliance is not the panacea it is considered to be. This is because the insider threat is far more complicated and nuanced: it is not merely a matter of 'not knowing' or 'refusing to act on knowledge'.

My co-authors and I have derived a taxonomy of insider threats called VISTA (inclusiVe InSider Threat tAxonomy), which enumerates seven different kinds of insider threat: (1) Untrained, (2) Fallible, (3) Disempowered, (4) Whistleblower, (5) Misbehaver, (6) Ideologue, (7) Malicious.

For the first category, training might well mitigate the risk. For the others, perhaps not. The second category includes the stressed and the burnt out, as well as those who make mistakes, a human tendency that is impossible to eradicate. What is needed in this case is for management to examine and reduce workloads, and to offer support to employees.

The whistleblower threat can only be reduced if the organisation implements an internal whistleblowing channel, and acts on reports to ensure ethical practice within the organisation.

The misbehaver knows what to do, but chooses to take shortcuts for a wide range of reasons. Engaging directly with the misbehaver and working with them to resolve these behaviours is likely to be far more effective than retraining.

While the misbehaver does not go out of their way to hurt the organisation, the ideologue and malicious insiders do, and no amount of awareness training and compliance mandates will make any difference. Here, the organisation is dealing with someone who actively intends to harm the organisation. As such, access control measures should be used to limit their ability to inflict damage. Managers, too, should be alert to signs of discontent so that these two insider types can be monitored and deterred before they decide to act.

The Disempowered category is an AI era category where strict compliance can actually be harmful. Because attackers now benefit from generational AI tools, exploits evolve at warp speed. Policies, being formulated based on past exploits, cannot help employees to spot new exploits. Organisations have to train employees to spot new exploits, and not use policy dictates to restrict their options.

I would welcome feedback and thoughts about our taxonomy. A link to the paper and a video are below.

Some links: Taxonomy paper
https://www.sciencedirect.com/science/article/pii/S0378720623001258
YouTube video: https://www.youtube.com/watch?v=xTHz4QBeq2M