

Four types of employees who are potential insider threats

March 28 2018

Academics have identified four types of employees who can become a threat to their companies – and explained the reasons why their workplace behaviour declines.

Researchers from the Universities of Glasgow and Coventry found organisational change within a company can act as an important trigger prompting even loyal and longstanding employees' behaviour to worsen.

The results of this range from time-wasting in the office to giving away confidential business information to competitors.

They identified types of employees—omitters, slippers, retaliators and serial transgressors – who carry out this 'counterproductive work behaviour' and the factors which cause it, in their new report.

Their findings have been used to create a series of resources to help employers manage organisational change and to try to prevent this behaviour by staff.

The project – funded by the Centre for Research and Evidence on Security Threats (CREST) – collected data from a company undergoing organisational change.

The research, by Professor Rosalind Searle and Dr. Charis Rice, involved interviewing managers and employees, reviewing HR and security paperwork relating to insider threat cases and carrying out

anonymous surveys within the organisation.

Their work revealed negative impacts of organisational changes – such as unpredictable working environment, inadequate communication, inconsistent leadership and unfair changes or processes—can cause distrust to form among employees and their managers.

This reduces people's psychological attachment to their companies and makes them more likely to carry out behaviour that makes them an insider threat.

The four types of employees who could potentially become an insider threat to their company are:

- **Omitters** – These are people who carry out this behaviour through an incapacity to effectively self-regulate their actions. They unintentionally breach rules and need help from colleagues to reduce the insider threat risk they present.
- **Slippers** – These are employees who occasionally undertake single acts of counterproductive work behaviour, such as taking home 'on-site only documents' or being rude to others.
- **Retaliators** – These are employees who deliberately undertake small acts designed to harm the organisation. Over time, if unchallenged and uncorrected, these can cause problems for colleagues and create additional costs and risks for their employers.
- **Serial Transgressors**—These individuals undertake a wide array of counterproductive work behaviour which undermines the authority of management and increases the security risks of those they work with.

But Prof Searle and Dr. Rice say managers can help reduce this behaviour by introducing the five core skills

These are: being fair and consistent with HR procedures and people during times of change; creating a system of organisational citizenship in which reporting counterproductive working behaviour is considered a protective measure rather than a punishment; communicating change initiatives transparently, consistently, regularly and collaboratively; adapting change initiatives in response to assessments of individual, team and organisations vulnerability; and managers leading by example.

Dr. Charis Rice, from Coventry University's Centre for Trust Peace and Social Relations, said:

"There are many examples of high-profile companies which have made the headlines following [employee](#) sabotage. It is vitally important to understand how these situations come about: the types of employee who might resort to these behaviours; why it happens and how managers' actions can prevent this happening.

"Our aim was to provide a framework to predict, identify and mitigate counterproductive work behaviour and insider threat within the context of organisational change.

"We found examples of team and managerial distrust that led to employees withdrawing their effort from organisations and in some cases even bred revenge [behaviour](#)."

Prof Rosalind Searle, from the Adam Smith Business School at University of Glasgow, said:

"Critically, our results showed that such outcomes were often an unforeseen consequence of an existing 'need to know' security culture and in part, the perceived heavy-handedness of HR and security teams with whom staff felt reluctant to share concerns."

More information: The resources are available to view at crestresearch.ac.uk/cwb

Provided by Coventry University

Citation: Four types of employees who are potential insider threats (2018, March 28) retrieved 25 April 2024 from <https://phys.org/news/2018-03-employees-potential-insider-threats.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.