PAUL MARTIN

TEN TOP TIPS ON INSIDER RISK

Paul Martin's textbook, *Insider Risk and Personnel Security* (Routledge, 2024), explores the nature and origins of the problem (insider risk) and the means of tackling it (personnel security). This article attempts to distil the complex issues into a set of ten simple principles.

We often think of security as protecting us from bad things in the world outside. But the worst risks can come from within. They stem from insiders – people who betray our trust – and they require a different sort of security response. Human behaviour lies at the heart of these risks, making them the most interesting of all security problems. Insiders have been found in every type and size of organisation, from small tech start-ups to multinational corporations and government departments.

1 IT CAN GET PHYSICAL

Despite the impression created in some academic literature, insiders do more than just compromise cyber security. Insiders can inflict harm in varied and imaginative ways, including physical sabotage and violence. For example, trusted insiders have assassinated political leaders and suicidal airline pilots have deliberately crashed planes, killing everyone on board. It remains a notable factoid that whereas many hundreds of people have been killed by insiders, no one has (yet) been killed as a direct consequence of a cyber attack, as far as we know.

2 BEWARE OF THE (UN)KNOWN UNKNOWNS

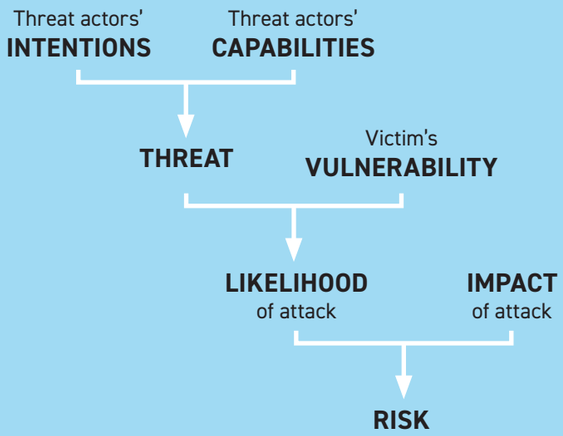
Insiders are capable of causing more harm than external threat actors because they already have legitimate access, know more about their victim, and may have authority over others. With the exception of the truly unwitting insider, they also behave covertly. The most capable insiders remain undiscovered for years and some may never be found. The history of espionage is littered with examples of enormously damaging spies who have operated in plain sight within high-security organisations for decades. The visible manifestations of insider risk are therefore only the tip of an iceberg of unknown size. This means, among other things, that the number of known insider cases within an organisation is a bad metric of insider risk. What it really measures is the ability to detect the problem. The absence of known cases is not evidence of absence of risk.

> **...the number of known insider cases within an organisation is a bad metric of insider risk.**

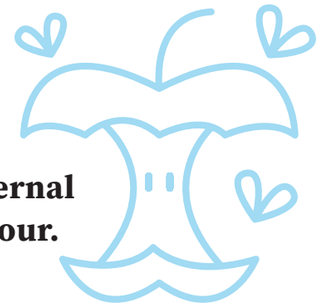
3 THE RISK IS DYNAMIC AND ADAPTIVE

In common with other types of security risk, insider risk is dynamic and adaptive: the risk changes over time and it adapts in response to the defensive actions of potential victims. Intentional insiders are intelligent threat actors who find ways of defeating security and remaining undetected. In some cases, their ability to do this is enhanced by support from a sophisticated external threat actor such as a hostile state agency. For personnel security to work effectively, it too must be dynamic and adaptive. This requires, among other things, agile mechanisms for discovering risks and genuinely learning lessons (as distinct from merely *identifying* lessons, which is all that many bureaucracies do).

The causal chain that generates insider risk and other security risks (Martin, 2019):



> **It falsely implies that insider risk is an inherent property of the individual, ignoring the crucial influence of work and home environments and other external factors in the genesis of insider behaviour.**



4 STRATEGY EATS CULTURE FOR BREAKFAST

Culture is important, of course. But a bigger barrier to effective personnel security in many organisations is a basic lack of strategic purpose. Personnel security should be an integrated system of complementary capabilities designed to achieve strategic outcomes like reducing risk, building trust and strengthening organisational resilience.

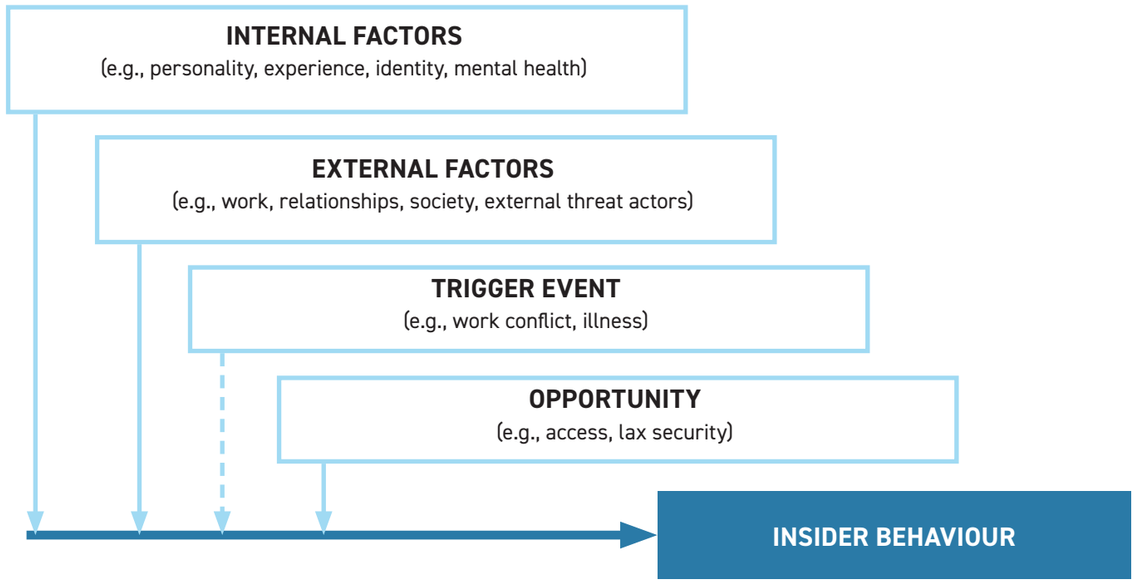
In practice, however, it is often a motley assortment of policies and processes that have accumulated over time, with little evidence base or strategic underpinning. Personnel security regimes that lack any explicit purpose or strategy tend to under-perform.

5 FORGET THE ROTTEN APPLES

Insiders are often portrayed as the few 'rotten apples' who lurk within an otherwise trustworthy workforce. The 'rotten apple' metaphor is deeply flawed, however. It falsely implies that insider risk is an inherent property of the individual, ignoring the crucial influence of work and home environments and other external factors in the genesis of insider behaviour.

It encourages a binary approach (trusted worker or rotten apple) to a risk that varies along a continuum. It also provides ammunition for marketeers who sell technologies that purportedly locate the 'rotten apples' through their behaviour on digital networks.

A simple model showing how internal factors, external factors, trigger events and opportunity combine in the development of insider behaviour (Martin, 2024):



6 PREVENTION IS BETTER THAN CURE

The ideal way to manage any security risk is to stop it from materialising, rather than waiting for bad things to happen and then dealing with the symptoms. The same is true for insider risk. Personnel security should aim to detect the weak early signals of potential insider risk and stop it developing into full-blown insider behaviour.

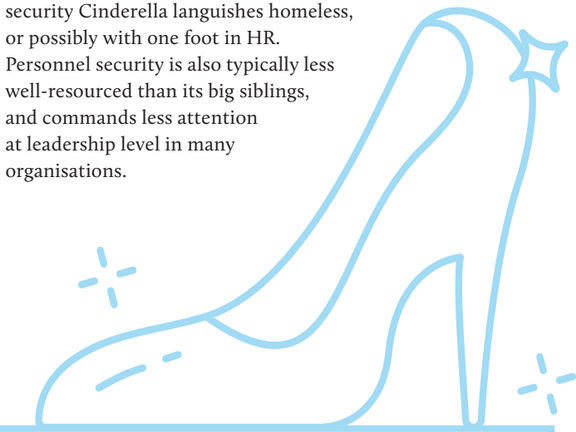
> **Personnel security should aim to detect the weak early signals of potential insider risk and stop it developing into full-blown insider behaviour.**

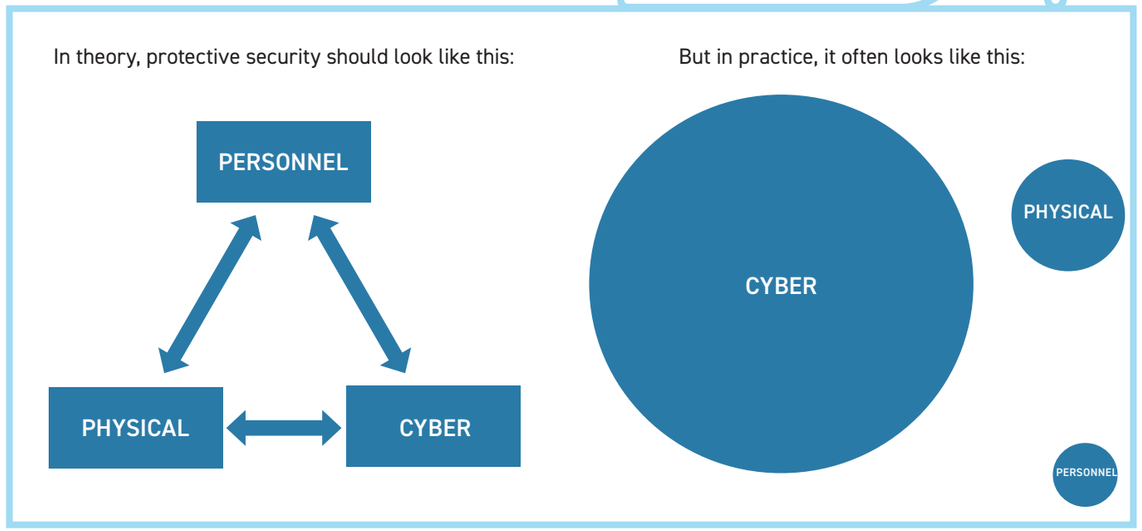
One way of doing this is through a welfare approach, in which the organisation seeks to help individuals with whatever problems might be nudging them onto the developmental path towards insider action. Most people are never going to become harmful insiders, and reaching for punitive action at the first sign of trouble is rarely the right answer.

7 RESPECT CINDERELLA

A central doctrine of protective security states that physical, personnel and cyber security are hugely interdependent and should therefore be managed holistically. A well-placed insider can defeat most physical or cyber security defences; cyber attacks can facilitate insider attacks; physical and personnel security measures are needed to protect cyber systems; and so on.

Nonetheless, many organisations have security structures that are far from holistic, with cyber security sitting in one silo and physical in another, while the personnel security Cinderella languishes homeless, or possibly with one foot in HR. Personnel security is also typically less well-resourced than its big siblings, and commands less attention at leadership level in many organisations.





> **Trust is the universal currency of insider risk and personnel security.**

8 IT'S ALL ABOUT TRUST

Trust is the universal currency of insider risk and personnel security. An insider can be defined as a person who betrays trust by behaving in potentially harmful ways: they have been trusted by an organisation, which gave them access to its assets, but they abuse that trust by behaving badly and potentially causing harm, whether intentionally or unwittingly. Arguably, the purpose of personnel security is to reduce insider risk and build trust by ensuring that people who have been trusted are trustworthy and remain trustworthy.

The four essential components of trustworthiness (after Martin, 2024):

The components of trustworthiness	
BENIGN INTENTIONS	**INTEGRITY**
COMPETENCE	**CONSISTENCY**

9 THERE ARE NO SILVER BULLETS

It might be tempting to believe that a single process or piece of technology, such as an automated monitoring software package or pre-employment screening, can deal with insider risk. Tempting but wrong. Both in practice and in principle, no single process or technology by itself can ever be an adequate defence against insider risk. Personnel security requires defence in depth from a system of complementary measures.

The fundamental reason is that insider risk – in common with many non-trivial problems – is an emergent property of a complex adaptive system. Systems problems require systems solutions, not silver bullets.

A simple model of a personnel security system (Martin, 2024):

10 WORDS MATTER

Terms such as 'insider' and 'vetting' have many different definitions, creating ample scope for confusion. For instance, 'vetting' can be synonymous with personnel security in its broadest sense, or it may refer only to pre-employment screening. The two are very different. 'Insider' is also fraught with ambiguity. The previous CPNI definition ('a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes') meant that 'insiders' were the small minority of people who presented a heightened risk.

In contrast, the new (2023) NPSA definition classifies literally everyone with current or previous authorised access as an 'insider'. Both definitions are legitimate, but they have very different meanings. We should spell out what we mean when using these words.

Paul Martin CBE is Professor of Practice at Coventry University's new London-based Protective Security Lab and a Distinguished Fellow of RUSI. He has more than 30 years' experience as a practitioner in the national security arena. He is a former head of CPNI (now NPSA) and a former Director of Security for the UK Parliament.