Unsurprisingly, the topic of Insider Threat is an unpalatable topic for most businesses, as the natural tendency is to assume that our colleagues do not wish to cause the organisation harm. While this may have been the case historically, digital innovation and the interconnected world expose tangible and intangible assets in a way never experienced before.

Numerous incidents of employees causing harm from within have been recorded ranging from the theft of intellectual property, the compromise of trade secrets and the misappropriation of financial assets to technology sabotage and beyond. Of these incidents, some have been deemed accidental while others have been intentional and attributed to full-time members of staff. In fact, the UK Centre for the Protection of National Infrastructure conducted research in 2013 and found that an Insider act was 88 per cent more likely to be carried out by a headcount member of staff, citing the two most frequent types of Insider activity as unauthorised disclosure of sensitive information (47 per cent) and process corruption (42 per cent). Indeed, the EU Agency for Network and Information Security reported in August this year that the most expensive attacks are those orchestrated by an Insider and this appears to be accurate considering that the estimated cost of intellectual property and trade secret compromise by the Detica Report on the Cost of Cybercrime in 2011 is £9.2bn per year. With meaningful, peer-reviewed data becoming available regarding the theft, compromise and loss of organisations’ crown jewels, there is arguably a greater requirement than ever for business leaders to mitigate Insider Threat as part of their enterprise risk strategy, to secure their market reputation, protect their brand and remain competitive.

The cost
Protection of assets should not be cost-prohibitive. There is a balance between business enablement and business protection. Consideration of the threat posed to an enterprise’s crown jewels is based on knowing what they are and who has access. Whether digital or physical, trade secrets are hugely valuable and must be protected from internal compromise, particularly as they have no dedicated protection in criminal law in many jurisdictions. Insider Threat is not a technology problem; while systems within have been recorded ranging from the theft of intellectual property, the compromise of trade secrets and the misappropriation of financial assets to technology sabotage and beyond. Of these incidents, some have been deemed accidental while others have been intentional and attributed to full-time members of staff. In fact, the UK Centre for the Protection of National Infrastructure conducted research in 2013 and found that an Insider act was 88 per cent more likely to be carried out by a headcount member of staff, citing the two most frequent types of Insider activity as unauthorised disclosure of sensitive information (47 per cent) and process corruption (42 per cent). Indeed, the EU Agency for Network and Information Security reported in August this year that the most expensive attacks are those orchestrated by an Insider and this appears to be accurate considering that the estimated cost of intellectual property and trade secret compromise by the Detica Report on the Cost of Cybercrime in 2011 is £9.2bn per year. With meaningful, peer-reviewed data becoming available regarding the theft, compromise and loss of organisations’ crown jewels, there is arguably a greater requirement than ever for business leaders to mitigate Insider Threat as part of their enterprise risk strategy, to secure their market reputation, protect their brand and remain competitive.

Insider Threat is not a technology problem; while systems within have been recorded ranging from the theft of intellectual property, the compromise of trade secrets and the misappropriation of financial assets to technology sabotage and beyond. Of these incidents, some have been deemed accidental while others have been intentional and attributed to full-time members of staff. In fact, the UK Centre for the Protection of National Infrastructure conducted research in 2013 and found that an Insider act was 88 per cent more likely to be carried out by a headcount member of staff, citing the two most frequent types of Insider activity as unauthorised disclosure of sensitive information (47 per cent) and process corruption (42 per cent). Indeed, the EU Agency for Network and Information Security reported in August this year that the most expensive attacks are those orchestrated by an Insider and this appears to be accurate considering that the estimated cost of intellectual property and trade secret compromise by the Detica Report on the Cost of Cybercrime in 2011 is £9.2bn per year. With meaningful, peer-reviewed data becoming available regarding the theft, compromise and loss of organisations’ crown jewels, there is arguably a greater requirement than ever for business leaders to mitigate Insider Threat as part of their enterprise risk strategy, to secure their market reputation, protect their brand and remain competitive.

In the digital age organisations must learn to protect their assets from theft, sabotage and compromise – even by their own employees.