Picture credit: AdobeStock

INSIDER THREATS

Miguel Clarke *underlines the potential damage that can be caused to your organisation's cyber security by a 'wild card'*

As cyber attacks escalate globally, organisations face growing challenges not just from external threats, but also from insider risks. With insider threat incidents surging by 44 percent in the past two years and the financial toll reaching a staggering $15.38-million per breach, the need for proactive security measures is greater than ever. This article discusses the critical role of leadership, employee morale and cross-departmental collaboration in combating these unpredictable, yet damaging, internal risks.

With the number of cyber attacks at an all-time high, causing billions of dollars in financial losses globally, organisations are facing unprecedented risks. From small businesses to large multinational corporations, the rise in sophisticated cyber threats has made it clear that no organisation is immune to the threat of data breaches, consequential reputational damage and not to mention costly legal ramifications.

However, it is not just external actors that need to be defended against. One of the most unpredictable and damaging cyber security risks organisations face today is insider threats. Originating from individuals who already have access to an entity's systems and data, insider threats can be inherently more challenging to detect and mitigate. These threats may stem from current or former employees, contractors or business partners who have, or have had, authorised access to the organisation's systems, networks and sensitive data.

Poor cyber security hygiene significantly amplifies the potential for destruction to an organisation

Recently published data provides real insight into the scale of the problem faced. In the last two years alone, there has been a 44 percent surge in insider threat incidents, with the average cost of each incident reaching an eye-watering $15.38-million. More alarmingly, between 2019 and 2024, the number of organisations reporting insider incidents has grown from 66 percent to 76 percent – that's nearly three-quarters of all organisations grappling with this issue. Insider threats generally fall into three distinct categories.

The first is malicious insiders who intentionally misuse their access for personal gain or to inflict harm on the organisation. These are often disgruntled employees or individuals who may be seeking financial gain, revenge or are working in collusion with external actors.

The second is negligent insiders, those who inadvertently compromise security through carelessness or lack of awareness. External actors, such as hackers, can exploit weak security practices or vulnerabilities to turn outsiders into insiders. Poor cyber security hygiene significantly amplifies the potential for destruction, with organisations that maintain strong security practices experiencing 35 times fewer destructive ransomware events.

The final type of insider threat is compromised insiders: individuals who have been coerced or manipulated by external actors into actions that jeopardise the organisation that employs them. This can occur through methods such as phishing, blackmail or social engineering – where attackers take advantage of vulnerable individuals to carry out malicious activities on their behalf.

It is important to remember that when it comes to insider threats and cyber security in general, there is no stereotypical perpetrator. As such, detecting insider threats is a real challenge, but there are several factors that organisations should consider and monitor closely.

The first is the length of employment. Notably, 38 percent of employees involved in dishonest behaviour have been with their organisation for less than a year, suggesting a higher risk-taking propensity early in employment. Taking this one step further, 75 percent of those recorded for unlawful data acquisition or disclosure have been employed for under five years.

That's not to say that longer-term employees are not exempt from risk. A striking 80 percent of those involved in bribery cases have been with their organisation for over ten years. This could be triggered by personal grievances, a sudden change in financial or personal circumstances or simply disillusionment with the company direction.

Vigilance is key when it comes to insider threats, and there are many 'red flags' that may give an indication of malicious intent. The first is unauthorised or suspicious data access and handling; this includes accessing sensitive information or systems without a legitimate need to know. Downloading, copying or transferring large amounts of data, attempting to bypass security controls or access restrictions and the unauthorised use of removable media or external storage devices should also be considered unusual and a potential security risk.

The next category is information technology misuse, such as installing unauthorised software, exhibiting unusual network activity, excessively using personal email or cloud storage for work, or experiencing frequent password resets or account lockouts.

Other categories include disgruntled or disruptive behaviour from staff, suspicious communications – perhaps with foreign entities or competitors, the use of encrypted or anonymous communication channels or even attempts to circumvent communication monitoring or surveillance systems.

Personal or financial issues are also something to look out for. Sudden or significant changes in lifestyle or spending habits, involvement in illegal activities or substance abuse, and financial difficulties such as debt or gambling problems can all increase an individual's risk profile.

SOMETHING THAT MUSTN'T BE OVERLOOKED IN THREAT PREVENTION IS EMPLOYEE MORALE

So, in addition to remaining vigilant, how can organisations successfully protect themselves against insider threats? In every insider threat case, there is a combination of network activity and employee behaviour. In other words, the malicious activity crosses both physical and electronic modalities.

Successful insider threat programmes require a multi-disciplinary team (MDT) approach involving individuals from across the organisation, responsible for physical security, cyber security, operational technology, information technology, HR and legal.

Monthly meetings of the MDT play a pivotal role in protecting organisations from insider threats, developing a strategy to support early threat detection, enable effective mitigation and ensure an appropriate response to anomalous behaviour.

Collaboration between HR and IT is particularly critical here because it combines the strengths of both departments to create a comprehensive approach to security. By combining their expertise and resources, HR and IT can create a powerful synergy that significantly reduces insider risk. The HR department has deep insights into employee behaviour, motivations and potential vulnerabilities. This knowledge can help IT security teams identify early warning signs of potential insider threats and tailor security measures accordingly. In addition, HR policies and practices can significantly influence the likelihood of insider threats. By working together, HR and IT can develop policies and procedures that foster a culture of security, promote ethical behaviour and discourage risky actions.

The employee lifecycle – starting from hiring practices to the working environment, training programmes and leadership quality – can significantly influence the likelihood of insider threats. Organisations should ask themselves: are we hiring the right employees? Are we providing adequate training? Does the organisation's culture encourage ethical behaviour or does it create an environment where malicious actions thrive?

Cultivating a culture of security and instilling a sense of responsibility and awareness among employees is crucial in the fight against insider threats. This should be complemented by a strong governance and risk management programme that establishes clear guidelines and procedures about expected behaviours, both online and in the workplace. A comprehensive employee manual coupled with robust employee onboarding and offboarding processes will also help to shape an informed and vigilant workforce.

THE RISE IN CYBER THREATS SHOWS THAT NO ORGANISATION IS IMMUNE FROM BREACHES

Something that mustn't be overlooked when it comes to threat prevention is employee morale and effective leadership. Insider threats are largely 'people problems'. That is, most companies do not hire 'bad actors', but over time relationships can sour due to unresolved conflicts, poor communication, or a lack of support, which can cause disengagement, resentment or even malicious intent.

Having interviewed many insiders during my time in the FBI, a common complaint was always about a leader's behaviour or how they were treated. While this does not justify unlawful behaviour, it is a reminder that good leadership always matters. Transformational leadership, which inspires and motivates employees while fostering a positive and supportive work environment, is probably the most powerful tool one can employ to safeguard the organisation and its data. Employee well-being programmes contribute not only to the overall welfare of the workforce, but also to the prevention of potential insider threats by addressing underlying issues proactively.

Employee training and education are also key factors in preventing insider threats, and organisations should implement regular, engaging cyber security training sessions for staff to stay abreast of the evolving technological landscape. Organisations must align security training with company culture, set clear expectations for both leaders and employees, and conduct regular training sessions to reinforce the importance of cyber security. Encouraging preferred employee behaviours and setting a positive tone from the top can go a long way in preventing insider threats.

The implementation of User Activity Monitoring systems (UAM), which continuously assess behaviours, is also hugely beneficial, enabling the early detection of employees with heightened risk factors. Similarly, Entity Behaviour Analytics (UEBA) provides insight into anomalous activities and helps in understanding data movement, which is another key step. By gaining insight into how data moves within an organisation, who accesses it, and for what purpose, potential risk areas can be identified. Identity Access Management (IAM) integration is also important, linking data flow analysis with identity and access management strategies to ensure appropriate access control and minimise the risk of data exposure.

Ultimately, the purpose of every information security programme is to maintain the confidentiality, integrity, and availability of said information. Insider threats are a formidable challenge to this and for organisations to mitigate, but with the right strategies in place and by adopting a proactive, multifaceted approach, the risk and impact of these 'wild card' threats can be reduced substantially ●

Miguel Clarke is GRC and Cyber Security Evangelist at Armour.

Disgruntled employees can misuse their access for personal gain or to inflict harm on the organisation