COMBATTING INSIDER THREAT: PUTTING PEOPLE FIRST

Are you confident that insider threat is at the centre of your cybersecurity strategy?

An investment in cybersecurity without accounting for insider threat is a strategy that is likely to fail. Around 60 per cent of G20 companies are expecting heightened threat from insiders[1], with the average global cost of insider threats reaching $11.45m[2] (£8.3m). Insider threats consist of connected users with trusted network access who can exploit systems which protect critical assets, exposing organisations to damaging reputational and economic effects, as well as intellectual property or commercially sensitive information loss.

The uptrend in threat is due to increased stressors as a result of the ongoing pandemic which, in turn, have exacerbated threats from insiders. When employees become stressed, isolated, or disenfranchised, the risk from insider threat rises. This, coupled with a remote work environment which often includes less oversight from leadership, whether perceived or realised, contributes to the growing risk.

Today's digital world has created additional opportunities for exposure, wittingly or unwittingly. Datasets, privileged company information, and user credentials are all of value to nefarious cyber actors. Due to numerous access points via platforms and apps, sensitive information is ever-more accessible. Some 68 per cent of organisations fear insider negligence from ignoring corporate policies[3], increasing the risk of being exposed or stolen by an insider, especially as people become the primary target of threat actors.

Capitalising on the pandemic and the move to digitalisation, cyber threat actors have launched newly targeted attacks focused on individual employees, outpacing current defence mechanisms. Inadvertent insiders, those who facilitate access to networks by falling for phishing or social engineering attacks, are being exploited by Covid-19 themed campaigns such as offering early vaccinations. Existing training and detection programmes are often outdated and fail to keep pace with the latest threats; for example, attackers actively recruiting insiders on the dark web[4].

How can business leaders mitigate the risk?

The first step is recognising all organisations have risk from insider threats and identifying ownership and accountability of the issue; it has recently been found that cybersecurity is increasingly becoming the responsibility of in-house legal departments[5]. What is vital to the current and future operating strategies of the organisation? How is this appropriately protected and managed? If organisations cannot answer these questions, it is difficult to determine the impact if your 'crown jewels' are compromised, and to demonstrate to stakeholders and external agencies that due consideration has been provided to appropriately secure sensitive information.

Ensuring insiders are a risk category covered in cybersecurity, and broader security, plans is a necessity. There is a tendency to spend more on sophisticated defence tools and overlook the human aspect of security. However, simple steps like implementing privilege settings, restricting user access to only the data required to do their job, can have just as great an impact. Another consideration directly impacting the risk of insider threat is employee morale[6]. Organisations should ensure their employees are engaged and content to minimise the likelihood of data theft or inadvertent leaks, especially during high-stress periods such as the global pandemic.

How will insider threat continue to evolve?

People are a central pillar of every organisation and therefore insiders will pose risks to valuable information they can access. This risk is heightened by a more remote and dispersed workforce likely to be an enduring consequence of Covid-19.

Whether low-level criminals or nation-states, cyber actors will continue to see people as a softer target than sophisticated network defences of an organisation, and using coercion or social engineering on personnel is emerging as an easier attack vector. When considering legal responsibilities for an organisation, too often the focus is on the outcome of an external cyber attack. This mindset overlooks the consequences of insider threat and leaves organisations vulnerable. It would be prudent for organisations to reassess their threat vectors, ensuring they have considered the risk of insider threat. Are you confident that your organisation or client has effectively quantified their insider threat risk profile?

1 FTI Consulting Resilience Barometer® Covid Edition 2 https://www.observeit.com/2020costofinsiderthreat/ 3 Haystax Technology, Insider Attacks Industry Survey 4 https://www.infosecurity-magazine.com/opinions/dark-net-recruitment-malicious/ 5 https://www.infosecurity-magazine.com/news/legal-teams-responsible/ 6 https://www.personneltoday.com/hr/how-covid-19-has-added-to-insider-threat-risks/