# Audit Committee update

## Insider threat

*As the cyber threat landscape evolves, boards should continue to look for ways to oversee cybersecurity risk. Whilst much of the news coverage surrounds external cyber attacks, in fact, 44% of data breaches are attributable to insiders. When examining the characteristics of an 'inside threat', the* ***US State of Cybercrime Survey, with PwC as one of the co-sponsors*** *found that only:*

**10%** exhibited disruptive workplace behaviour

**8%** had received formal warnings/undergone disciplinary action

**7%** were labelled as poor performers in reviews

This means that 90% of 'insiders' displayed no worrying characteristics prior to their attacks. Perhaps more surprisingly, 80% of attacks are committed during work hours on company issued software. In the same survey, our research found that 16% of those asked committed their crime for financial gain and 10% for revenge. Inside data breaches can have a significant impact on a company, including a drop reputation, a loss of customer and revenue, uncertainty and a drop in share price, as some of the high profile cases have shown. Therefore, how can companies address the issue and mitigate the risk? There are some very basic principles which any company can adopt in order to address the issue:

**Get compliant** – ensure that all employees/third party contractors have the appropriate level of access to data/ programmes required. Access to certain systems may have built up for long term employees which may no longer be applicable.

**Stay compliant** – put in a process to ensure that access is regularly reviewed and actioned.

**Analyse** – use the data to identify anomalies and high risk users, especially third parties and contractors.

**Enhance** – identify high risk users and those who have gathered access and action a process to trim down these entitlements.

While trying to prevent a data breach may not be easy based on the lack of behavioural changes to an employee (based on 90% of insiders not showing any concerning characteristics) putting these actions into place will make it more difficult for a potential insider threat to carry out an attack. They will also improve an organisation's ability to respond quickly in the event of an insider attack.

pwc

Our cyber team have seen a number of ways in which companies are addressing insider threat, by using certain technologies such as identification of high risk users, dashboards that facilitate efficient management oversight, flight risk and behavioural analytics to predict likely threats. Not only is technology playing an important role in tackling insider threat, but culture and people are equally important. Companies who are embedding the right culture are aligning roles to the correct access requirements, providing training and awareness programmes, empowering their people to challenge when something doesn't seem right and understanding the common motivations and indicators which would push an individual to commit a data breach. Introducing the right technology and organisational culture can have a huge impact on mitigating insider threat.

We have produced a number of questions for the board to ensure that the right person is responsible for good access governance firm wide.

| CEO | CIO | CFO | HR Director |
|---|---|---|---|
| Who is in charge of insider threat management? | | | |
| What departments or functions are involved in handling insider threats? | | | |
| What are other companies doing to manage and mitigate insider threats? | How many detected security incidents are attributed to insiders?<br>Do we know who are our high risk users? | What is the impact of insider incidents? | How do we assess potential and existing employees and third parties for insider risks?<br>Does a safety culture exist in terms of:<br>• Awareness of insider threat?<br>• Challenge and questioning?<br>• Behavioural reviews? |

## Contacts

***Richard Mardling***
Director – Identity and Access Management
E: richard.w.mardling@pwc.com

***Emma Hunwick***
Cyber Security
E: emma.hunwick@pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.