Picture credit: AdobeStock

INSIDER THREAT

Noah Price *examines the risks employees can pose and how to prevent them*

If asked to describe a physical security breach that can impact a company, most people would think of an external criminal intent on harming an organisation. But what if the attack comes from within? Perpetrated by someone you should be able to trust? Insider threats are a serious security risk that every business must prepare for. Failing to do so could be reputationally or financially damaging. According to G4S's first-ever World Security Report, internal threats are expected to increase next year, with 92 percent anticipating their company will be targeted.

Threat actors who commit an insider threat are usually classified as a 'knowing insider' or an 'unknowing insider'. A knowing insider is someone who deliberately uses their access on purpose to cause harm. They are often motivated by financial gain. Or, sometimes they steal company data to gain a competitive edge. Usually, they are a lone wolf who acts on their own without any other influences.

An unknowing insider is someone who may not fully understand what they are doing, or becomes an Insider threat by mistake. Unknowing insiders can also be unaware that they are being taken advantage of by others. They might download malware, give information to scammers or click on a link in a phishing email.

Concerningly, internal threats are increasing. 89 percent of CSOs say their company experienced some form of internal threat in the last 12 months according to the World Security Report; this is expected to increase to 92 percent in the year ahead. Misuse of company resources or data is the most common internal threat, with 35 percent having experienced this, followed closely by leaking of sensitive information at 34 percent. This threat is expected to become the biggest internal threat in the next 12 months.

"Misuse of company resources or data" has the strongest correlation with "implementing more effective security." This was the internal incident most likely to drive companies to improve their security in the last year.

"Unauthorized access to company resources or data," "industrial espionage" and "intellectual property theft" are all expected to increase in the next year. Perceived financial gains may entice a company employee to share confidential information in exchange for payment. Insider threats make headlines; news outlets regularly report on high-profile or unusual incidents - which can damage a brands reputation in the media, with customers and stakeholders.

Fostering a culture that combines security awareness alongside up-to-date equipment and technology is the best preventative measure when it comes to preventing an insider threat. Employees should be regularly trained to identify phishing attempts and suspicious behaviour, as well as reminding them of data security protocols. They should also only have the access they need to certain documents and areas of a building.

Additionally, implementing strong access controls restricts digital and physical theft or leakage. Ideally, access controls should be enhanced with surveillance technology. When employees know the cameras are on them, it's harder to do anything deceitful. Cameras can also help with the issue of people using each other's access cards. The CCTV footage will show who actually entered any specific area, and exactly what they did there. Of course, CCTV will never be enough by itself but should be part of a full security system and monitored by a well-trained team ●

An unknowing insider may not fully understand what they are doing and become an insider threat by mistake

Noah Price is Academy International Director at G4S.