The Role That HR Departments Can Play In Defeating Insider Attacks

Are senior management becoming more distrustful of their staff or are they simply reacting to an undeniable fact: that 81% of all cybercrimes are carried out by insiders? And if this is the case, what are the implications for HR departments around the world?

A recent survey published in the Financial Times (31st October 2015) entitled 'The Global State of Information Security' found that in six major geographies around the world, including the UK, Germany, China, the US, Brazil and Europe, the respondents all listed 'current employees' as being the most likely source of a cyber-attack on their company, followed by 'former employees' in second place and then either 'unknown hackers' or 'competition'.

This finding is significant as it highlights the widening gulf between perception (that most cyber-crime is carried out by criminal gangs or rogue nation states) and reality (that most of it is, in fact, committed by current employees). This growing perception is probably the result of the disproportionate amount of press coverage given over to stories about external hackers and the financial and reputational damage that they can cause to companies. The recent TalkTalk hack here in the UK being one such example, with the company still counting the considerable costs of that attack - including the CEO yet to go before a House Of Parliament Select Committee where she can expect a - very public – grilling from the MPs.

Statistics published by a recent CPNI Insider Data Collection Study show that of these attacks, 88% are committed by permanent members of staff, 7% by contractors and 5% by agency personnel. The same organisation's definition of an 'insider threat' gives an indication as to why HR departments need to take the lead in combating this growing phenomenon or, at the very least, work more closely with their colleagues in the IT department.

An insider threat, according to the CPNI, can be defined as "the threat posed to an organisation from high risk behaviour of one or more employees, including contractors and business partners". If high risk behaviour by a member of staff presages a possible attack on his own her own company, then what steps can the HR department take to prevent this happening?

My recommendation is that it has to work in a much more collaborative way with the IT department. And here's the main reason why. For an attack to take place, the attacker must have the means, the motive and the opportunity.

Addressing the 'motive' aspect belongs firmly to HR departments which need to better understand why people commit these crimes and look out for the behaviours that could trigger them.

The 'means' and 'opportunity' belong squarely to IT departments which need to put in place more robust access management systems that prevent staff from going where they're not allowed to go, and cuts them off from the system when they themselves have left the company.

IT departments have much ground to make up in this area. For example, my company carried out some research recently into an important aspect of information security, namely identity and access. 50% of the respondents (who were IT professionals) that took part in our survey felt that it would be either 'difficult' or 'very difficult' to identify whether any ex-employees still had access via accounts to resources on their network. The same percentage (50%), thought the same about ex-third party providers accessing their network and an even bigger proportion (55%) thought the same about ex-contractors accessing their networks.

Managing 'orphan accounts' for businesses is clearly problematic. Research by YouGov found that 39% of of IT decision makers from large corporates took anything from a few days to a month to close a leaver's dormant account. But a disgruntled employee is unlikely to wait anything like that length of time before they start helping themselves to confidential company information.

In other words, their IT systems are simply not able to cope appropriately (i.e., swiftly) with staff leavers. So who's to blame here? Is this a problem with the IT Department's system, or the HR department's processes and procedures?

A truly effective solution is only achievable if the two departments work in tandem. The IT department's job is to put in place appropriate IT security systems and the HR department's job is to put in place the appropriate processes and procedures and create the right culture regarding the workforce's compliance or observance of them.

Compliance is key here and this area could prove to be the most difficult to achieve. A report by Raytheon (2015 Global Megatrends in Cybersecurity Report) found that one key attribution that was expected to 'worsen' (i.e., the security risk rating will increase) over the next few years was an 'inability to enforce compliance with policies'. In other words, companies will find it increasingly hard to make their staff follow their rules. And the tougher, more onerous or more strict the rules become, they less likely staff are to follow them.

Here are my six tips to help HR departments and IT departments jointly create a more 'holistic' approach to managing employee risk:

Work More Closely Together

It sounds obvious, but having a better understanding about each other's day to day work can help to identify and resolve many of the issues addressed in this article, e.g., leavers. Forming joint steering committees or creating other fora may help stimulate dialogues between the two departments leading to a more collaborative and effective way of working.

Re-Assess And Upgrade Existing Security Processes And Procedures

Many of these will have been in place for many years and will not address the relatively new phenomenon that cyber-security represents. When assessing them, ask yourselves these questions: Do they work in this new environment? Are they practical? Will they be observed? What are the consequences if they are not observed? What are the risks of non compliance and

is the organisation prepared to bear them?

Training

Make employees aware of the risks, and penalties, of a data breach and teach them how to spot it. Naturally, this training should involve both departments and should serve to demonstrate the new found cohesiveness between the two.

Create A More 'Vigilant' Culture

Most frauds are revealed by whistleblowers and an important preventative measure is to encourage a system and culture whereby employees can report anything unusual. Although unusual behaviour does not always presage a full blown cyber-attack, it might indicate that something is wrong.

Regularly Test Existing Systems, Processes And Procedures

Many former hackers are now gainfully employed trying to test the defences of companies that they formerly hacked into. (After all, they're best placed to know where the weaknesses are). The same approach can be adopted internally too.

Forget The Dichotomy Between Insider Threats And Outsider Threats

This demarcation line is rapidly blurring and is, in fact, disingenuous. Although the Talk Talk attack was carried out by external hackers, once they were 'in', they were able to make use of some lax internal controls to gain greater access.

Chris Pace, Head of Product Marketing at Wallix UK
Chris can be contacted at
cpace@wallix.com
www.wallix.com