Hewlett Packard Enterprise

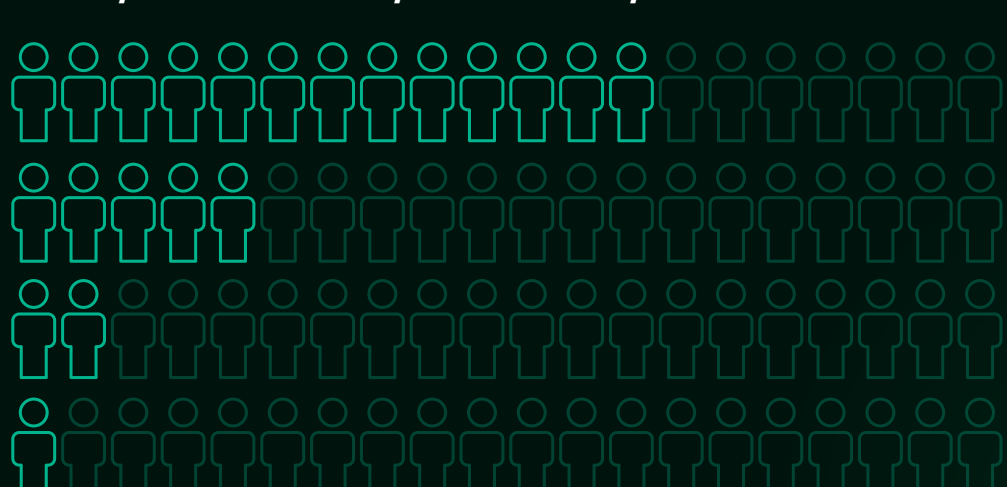
FireEye

CYBER SECURITY: THE DIGITAL ELEPHANT IN THE ROOM

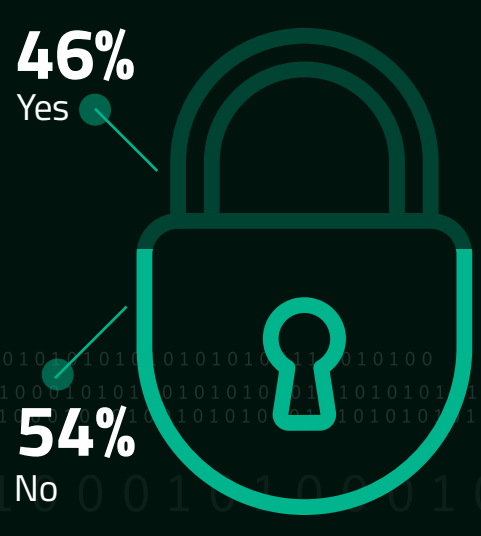
In a recent report, The Royal Society called for cyber security to become the primary concern for business, policy and research in the current climate, with heightened emphasis on information sharing and international collaboration.

As all elements of society are increasingly being lived out in the cyber domain, sensitivity around the threats posed by the plethora of attack methods and motives involved in cyber realms has been heightened. But just because we are aware of danger, does that mean we are doing enough to combat it or mitigate any fallout? In a survey of the energy sector conducted by Oil & Gas IQ, the answer would seem to be an alarming and resounding NO...

How long before you detect a cyber security breach?



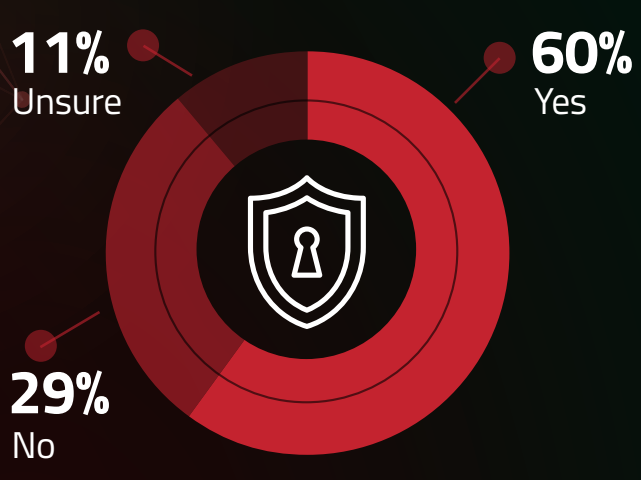
Do you know if you have been breached within the last year?



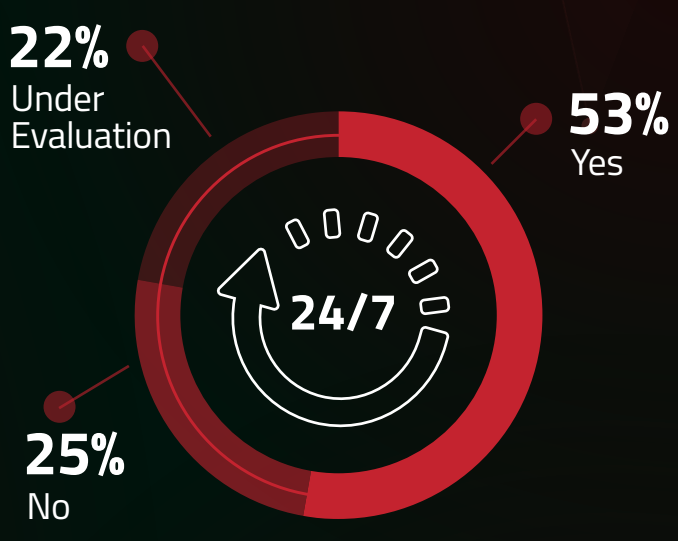
How do you assess impact/cost of breaches?

1 in 10 companies do not realise that they have suffered a significant cyber security breach for half a year. More than 50% of companies do not know if they have been breached in the past 12 months, nor how their companies assess the damage that has been done…

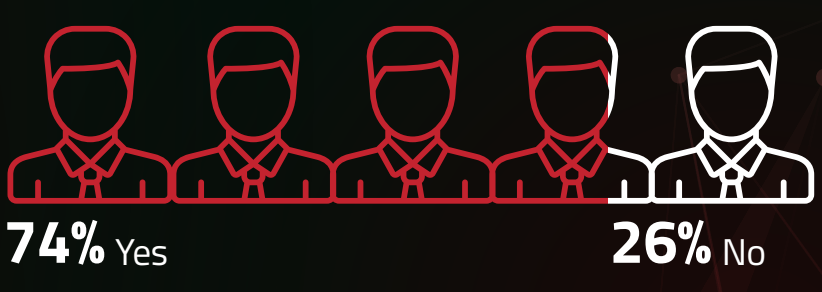
Do you know how often you are breached and how long before you detect it?



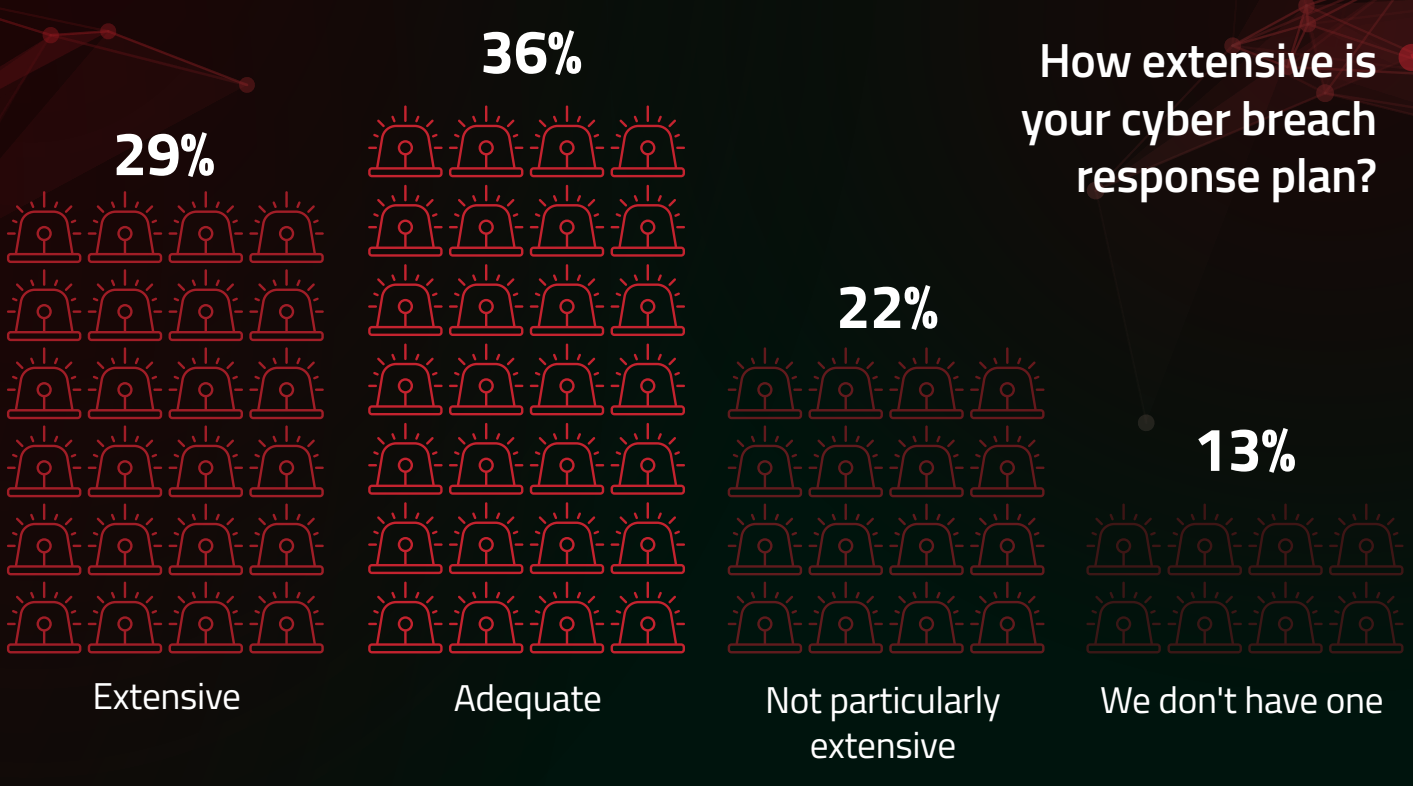
Do you have a 24/7 cyber security response plan?



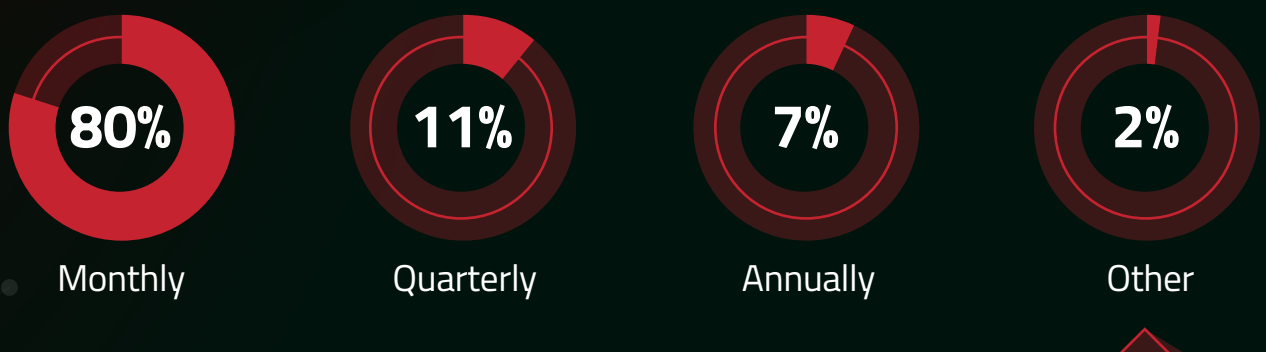
Does your cyber response plan have the support and inclusion of the board?



How extensive is your cyber breach response plan?



How often is your cyber response plan tested?



Almost **1 in 3** of companies surveyed do not believe that an adaptable cyber defence approach will give them a significant advantage over their direct competitors. Perhaps this is why **1 in 4** of them see no reason for the establishment of a 24/7 response plan to mitigate the effects of a cyber attack, and of those that do have a response plan, less than **1 in 3** believe it is all-encompassing and almost **1 in 10** only test this out on a yearly basis.

Out of 10, with ten as the highest rating, how would you rate the energy industry's capability to identify specific threat group activity and adapt strategy accordingly?

This would indicate that those inside energy companies rate their industry's ability to deal with cyber attacks as adequate but slightly below satisfactory.