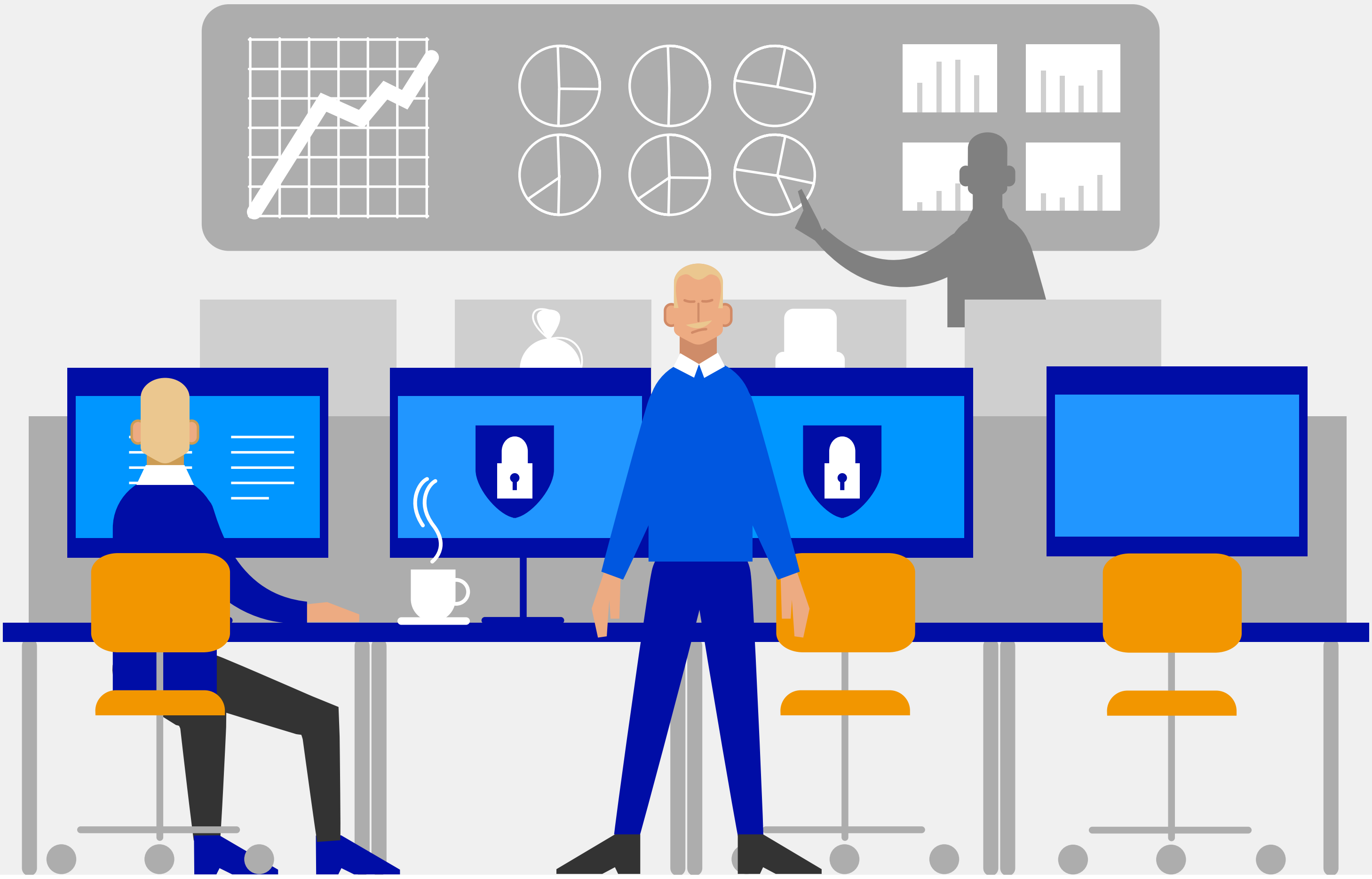
SPOTLIGHT ON UK IT DECISION MAKERS CYBER SECURITY PRIORITIES

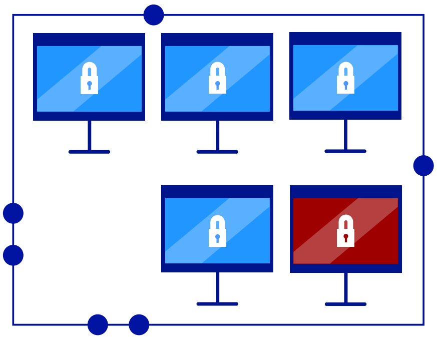
400 cyber security leaders and influencers across the UK shared with us their companies' priorities, challenges, strategies and budgets for 2020 and beyond. The results provide an insight into where IT decision makers are focussing their budgets to meet the challenges of a fast changing threat landscape, how COVID is driving rising cyber security spend, and the strategic importance of relationships between businesses and security providers.



Cubit TECHNOLOGY | F-Secure.

MOST BUSINESSES HAVE RECENTLY EXPERIENCED A CYBER ATTACK

Cyber security professionals work tirelessly to ensure that cyber attacks targeting their organisation are not successful. However, attacks are a growing inevitability, a fact that is highlighted by our research, which showed that three quarters of businesses experienced at least one attack in the last year. **One-in-five was attacked more than five times.**

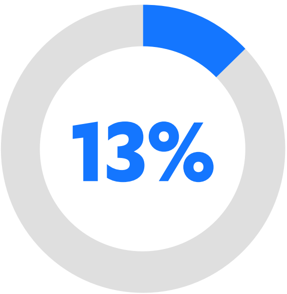


A RISE IN CYBER SECURITY SPENDING

To defend against these persistent threats most businesses are planning to increase their IT security budgets over the next year. More than a third say this increase will be between six and ten percent.

The COVID crisis has led some businesses to divert more funds into cyber security, with 13 percent of respondents stating that budgets are going to increase as a direct response to the challenges presented by the pandemic.

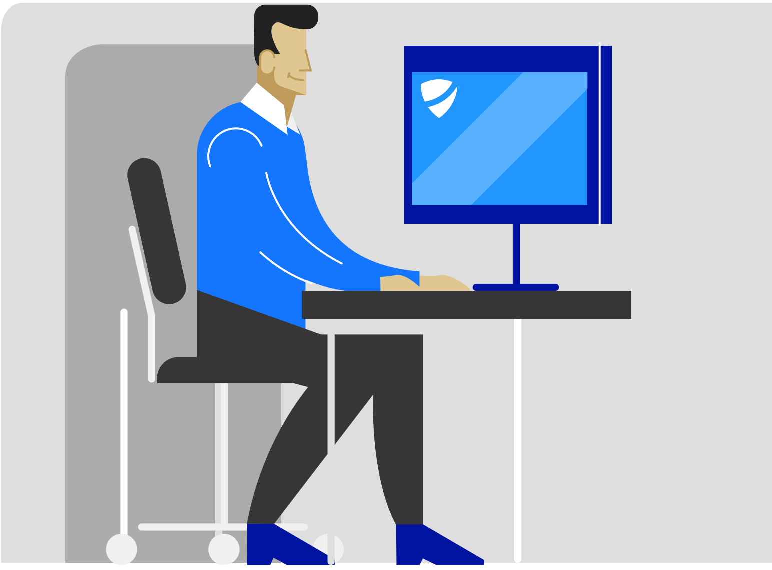
CISOs will undoubtedly welcome this boost to their budgets. The next step will be to research all available options to find the most robust defence possible in the face of a continually changing threat landscape.



FLEXIBILITY AND TRUST ARE KEY

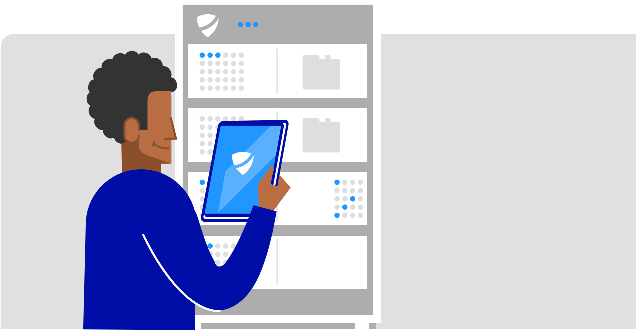
When purchasing a security product or a service, the majority of businesses (72 percent) want to pay monthly rather than annually, with a quarter looking for flexible contracts. This is likely to be influenced by economic uncertainty as businesses plan for further restrictions and changes due to COVID.

For those businesses opting to buy a solution through a service provider or reseller (26 percent), the most important factors are flexibility, clear and fair contracts, and trust. Businesses relying on an outside partner to help protect their IT systems must feel they can trust them, otherwise the relationship will quickly fall apart.



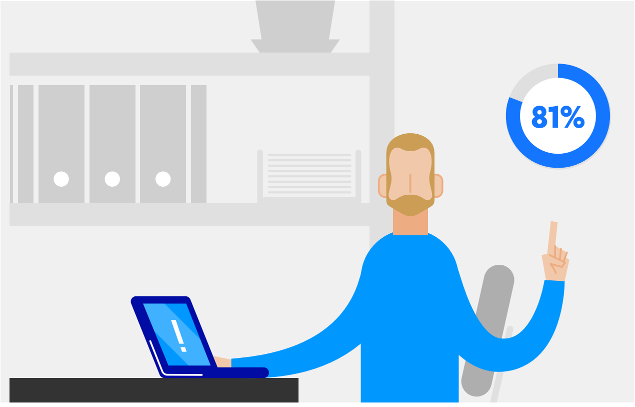
IN-HOUSE OR MANAGED SERVICE?

A majority of businesses still choose to manage most of their security solutions in-house. However, for smaller companies (with between 25-199 staff) the option of employing full time, in-house security specialists is often out of reach. In most cases they will choose the support of a managed security service. Only 38 percent of the smallest businesses have cyber security personnel, compared to 59 percent at the largest.



CYBER SECURITY SERVICE PROVIDERS ARE STRATEGIC PARTNERS

The research highlighted a close working relationship between in-house teams and outsourced security providers. An overwhelming majority **(81 percent)** of UK businesses with an IT service provider or reseller view them as a key or strategic partner. Many also heavily rely on their reseller or service provider for advice. Such a relationship is vital at a time when it is increasingly difficult to recruit and retain skilled cyber security professionals. It is predicted that the cyber skills shortage is only getting worse, making the role of the service provider as trusted advisor ever more important.

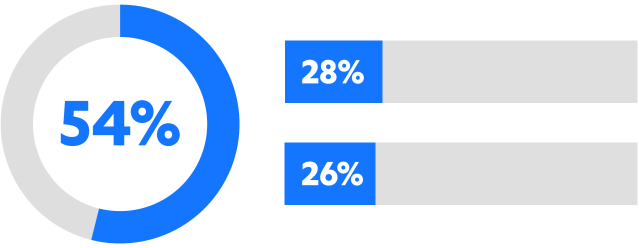


HOW EDR IMPROVES SECURITY

For the next 12 months the top priorities for IT decision makers are to prevent data breaches (28 percent) and malware or phishing attacks (26 percent). The most effective way to do this is to use Endpoint Detection and Response (EDR). More than half of respondents (54 percent) view EDR as a purchasing priority.

EDR augments endpoint protection solutions such anti-malware and spam filtering. If an attacker gets through the endpoint defences or they are not patched correctly, EDR is there to detect this and respond accordingly.

EDR solutions enable IT decision makers to achieve faster response times, better understanding and clearer reporting, which will lead to improved IT security.



ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We’re closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry’s best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world’s most potent threats.

Together with our network of the top channel partners and over 200 service providers, we’re on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

Cubit TECHNOLOGY | F-Secure