WHITE PAPER

CARBONITE® + WEBROOT®
opentext™ BUSINESS SOLUTIONS

Security awareness training remains a new, fast-growing category for MSPs

Introduction

For the last two years, we've reached out to MSPs using security awareness training solutions—ours or a competitor—with a brief survey regarding their use of cyber education to reduce security incidents and help their clients become more cyber-aware.

This November, we again surveyed 204 MSPs about their adoption of security awareness training (SAT), soliciting responses from current and former Webroot® Security Awareness Training customers spread across North America, Europe, the Middle East, Africa and Asia Pacific.

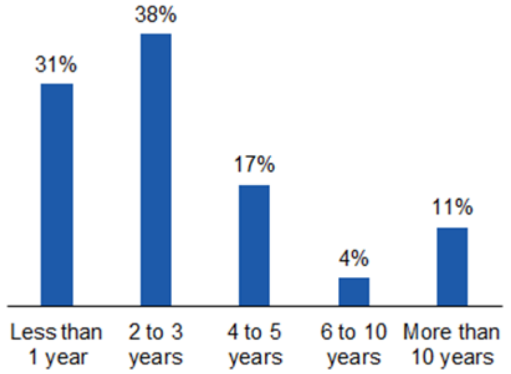
In this incentivized survey we asked:

- Is SAT use growing or declining?
- How do MSPs package training and offer it to their clients?
- How is SAT administered?
- What is the frequency of training? Do they target specific audience segments?
- What are some specific benefits and barriers to delivering SAT?

The 2021 survey results are in, and while adoption continues to grow, client reluctance remains the primary barrier again to SAT contributing to better IT security.

Now, let's take a closer look at this year's findings.

How long have you been offering Security Awareness Training (SAT)?

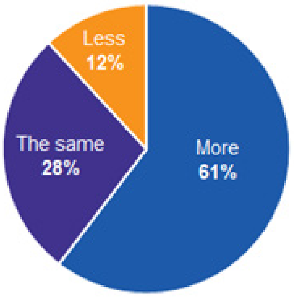


As we can see, of the 105 MSPs who responded this question:

- 69% have offered SAT for three years or less
- 31% have only offered SAT during the past year

This demonstrates a significant, ongoing growth in SAT offerings over the course of 2021.

Have you delivered more (or less) SAT in 2021?



52% of respondents provide SAT in 2021

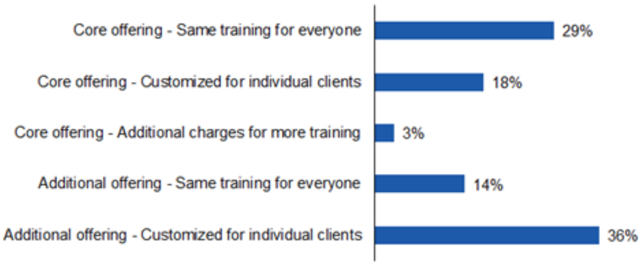
- AMER - 56%
- EMEA - 54%
- APAC - 37%

Increase from 46% that said they provided more training in 2020 (compared to 2019)

MSPs offered and delivered more training in 2021 than years prior, with 52% of respondents providing training compared to just 45% in 2020. Overall, 61% of MSPs say they delivered more training in 2021 compared to 2020, while only 46% of respondents in 2020 said they delivered more training in 2020 compared to 2019.

So, not only is training adoption growing, but it's also being used more regularly than before.

How do MSPs package SAT for their Clients?



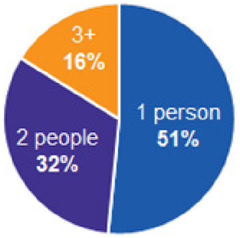
An important consideration is how MSPs package their training offerings. Two distinct approaches seem to have emerged:

1. For 29%, training is a core offering, where the same core content is used for every client

2. For 36%, training is an optional offering where training courses are customized by client

There's a clear split between offering training as a core offering versus as an add-on. From a revenue perspective, the 36% offering it as an add-on with customization suggests a potentially more lucrative approach to SAT.

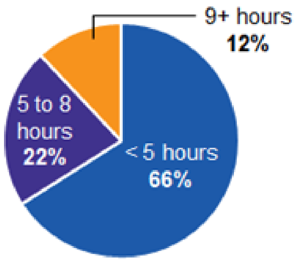
Number of staff involved in SAT administration?



Continuing in the vein of profitability, we see that 51% of the 96 respondents who answered this question needed only one person to administer SAT. A third used two people, and 16% had three or more personnel involved in administering their training.

We would add that a major focus of ours in the first half of 2022 is to make training and phishing campaigns more automated, reducing administrative burden and promoting profitability.

Monthly hours spent administering SAT?

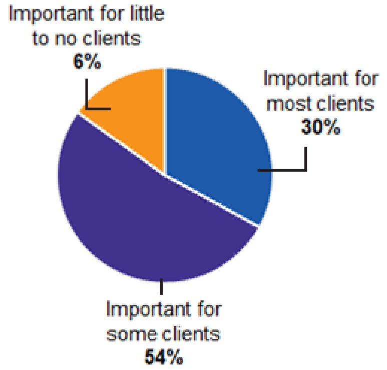


In addition to the limited personnel involvement, it was also interesting to see how little time is spent per month administering training.

In a normal 21-working-day month, 66% of MSPs spent less than five hours of time on SAT, while a further 22% spent only one day per month. Only 12% spend nine or more hours per month.

This suggests administration is not a large cost overhead in most cases. But unfortunately, small administrative overhead could also reflect a low frequency of training courses and phishing simulations delivered. (See 'How often do your Clients receive training?')

How important are compliance requirements to justify SAT?

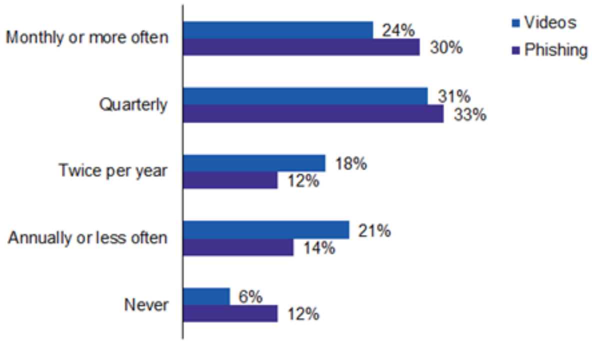


For 84% of MSPs, compliance is important.

This is to be expected thanks to stronger emphasis on SAT in cyber insurance requirements and cybersecurity frameworks like NIST.

This is also why we have made it a priority to include compliance courses in our flat-rate SAT pricing.

How often do your clients receive training?

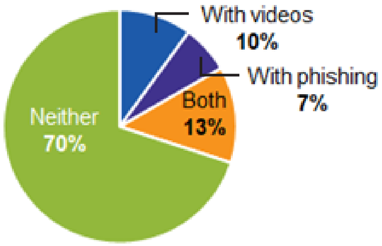


As in 2020, reported training frequency is less than ideal.

MSPs should probably shoulder as much blame as their clients do here. Our findings suggest that the ideal frequency for both training courses and phishing simulations is at least monthly. Only 30% of MSPs deliver phishing simulations this often, and less than a quarter push training course content at this cadence.

Frequency is important. Why? Because for SAT to change user behavior and genuinely raising cyber awareness, it needs to remain top-of-mind. Like all education, it's the sustained exposure to relevant, and high quality training content and phishing lures that produce results.

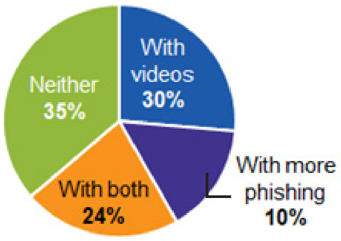
Do you target specific job roles?



Phishing attacks vary by job role, yet only 7% of MSPs are using job role to target their phishing simulations. A slightly higher 10% of MSPs are using job role to deliver relevant training content and 13% of MSPs are using job role to target both phishing and training.

These levels are low and show a missed opportunity to make cyber awareness training more targeted and effective.

Do you target simulated phishing victims?

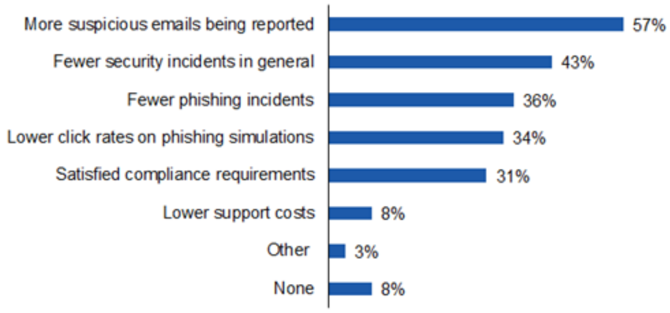


A useful technique to reduce phishing click rates is to target the users who click onphishing simulations with more training.

The aim is to raise their awareness of the consequences of thoughtlessly clicking email links in a way that's constructive and beneficial to their organizations.

It's interesting to see that 64% of MSPs do some extra training with phishing victims, and almost a quarter use both training course videos and additional phishing simulations to convey to high-risk users the dangers of phishing. If not overdone, this is a very valid tactic at reducing phishing click rates.

Have you or your clients experienced any benefits from SAT?



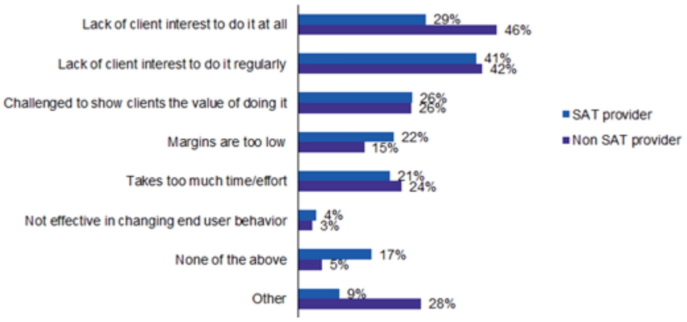
You could call this the "million-dollar" security training question. is SAT working for your clients?

The reported results, especially given the lack of continuous training delivered by most MSPs, are encouraging. They show that even a little training is a lot better than no training at all.

Almost 60% of respondents see an increase in user reporting as a result of training. This key when you consider the role email plays in introducing malware and business email compromise (BEC) attacks into organizations.

Furthermore, security incidents were almost halved, at 43%, with training. Both phishing incidents and phishing click-through rates were reduced by well over a third. Undoubtedly, these results would be even more impressive with more regular training.

Is anything preventing you from delivering more SAT?



MSPs responses here are split between those who offer SAT and those that don't.

For those providing training the top three issues are:

1. Lack of client interest in regular training (41%)

2. Lack of interest in training at all (29%)

3. Challenged to show the value of training (26%)

For those MSPs not offering SAT, almost half (46%) see a lack of client interest to do it at all and 41% see client willingness to do it regularly as the main barriers preventing them from offering training.

Summary: MSPs are underusing SAT

The main issue we see in the results of our survey is SAT being underused by MSPs due to insufficient buy-in from clients. Either they don't understand the benefits, have concerns about time spent training or are unwilling to pay a little extra for training. Of course, proving and clearly demonstrating the value of SAT is essential.

Consistent trends from this survey in both 2020 and 2021 reveal:

- It's still early – 69% of MSPs have only offered training for the past three years
- MSPs continue to split 50/50 between offering SAT as a core vs optional service
- MSPs know training is important. Only 4% believe it's ineffective in changing user behavior

Recommendations

Based on the survey's results, we recommend MSPs focus on three things in 2022:

1. Increase frequency of training to generate better data that demonstrates positive results

2. Simplify and position your service offering to address client concerns regarding productivity, costs and value, and to help with this we are producing a new paper that addresses those client concerns

3. Reduce administrative costs and increase training value by using automation features for campaigns and reports including auto-enroll, distribution lists, multi-course campaigns, reminders, and more

Contact us to learn more – Carbonite EMEA

Email: carb-salesemea@opentext.com

Phone: France: +33 (0) 1 47 96 55 41 | Germany: +49 2162 91980 20 | Netherlands: +31 73 648 1400 | UK: +44 333 1234 200

For all other countries please dial: +44 333 1234 200

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.