

Boost MSP Revenue and
Client Stickiness with
**SECURITY
AWARENESS
TRAINING**





At the rate Marvel Studios is expanding their film franchise, it's probably just a matter of time until they introduce an MSP superhero movie. Maybe with a catchy moniker like “Captain Invisible” or something similar...because the sad truth is, when MSPs are doing their best work it often goes unseen by their clients.

That's particularly true when it comes to your security services; while you are absolutely crushing it in terms of protecting your customers' businesses from cyberattacks, a remarkable thing happens—nothing.

Everything. Just. Works.

In an ideal world, delivering such superior protection would earn MSPs ongoing loyalty from their client base, yielding exceptional customer retention and long-term patronage—the “stickiness” that underpins every profitable and successful MSP. In reality, some clients may overlook your behind-the-scenes security heroics that keep their businesses running smoothly.

Happily, there's a solution that helps you enable even stronger cybersecurity protection for your customers—while adding a new revenue source and boosting client stickiness. When you provide Security Awareness Training (SAT) to your customers, you'll show them how to adopt the behaviors and best practices that thwart common cyberattacks such as phishing and ransomware. In the process, you'll gain a billable service and client appreciation for your high-visibility efforts.

This latter point should not be underestimated: for example, the cybersecurity behaviors your clients' employees learn will also carry over into their personal web surfing, email and social media activities, garnering you even greater recognition for the real-world security benefits you deliver as their MSP.

KEY CONSIDERATIONS WHEN EVALUATING SAT PROGRAMS



Superior Content

Make sure you can deliver enterprise-quality content for all of your clients, regardless of their company size.



Security Awareness in a Box

A complete program will include the perfect balance of phishing and behavioral remediation to identify at-risk clients, utilizing on-going simulations and continual reinforcement of best practices to effectively curtail their unsafe behaviors.



Simple Reporting

Automated reporting is a convenient tool that gives quick insights into how well your clients are doing in their efforts to reduce risk and build a cyber-secure workplace.



Automated Deployment

Helps maximize your SAT program's impact with minimal administrative effort; for example, look for phishing simulations that are rolled out in a periodic drip-style campaign.



Integrated Phishing Sims

Automated phishing simulations efficiently deliver key metrics, delivering monthly reports on how your clients are improving, and they help to demonstrate your service's ROI to them.



Effective and Concise Delivery

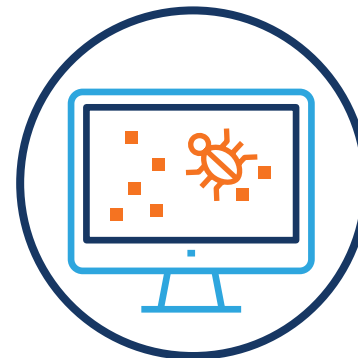
Insist on programs that provide easily consumable, time-conscious and proven topics which enable your clients to learn core security awareness practices in a minimal amount of time.

EXPLAINING THE VALUE OF SAT TO YOUR CLIENTS

STEP 1

Clearly identify the problem you're trying to solve

Discuss with clients why you think SAT could benefit them. It might be because they suffer from phishing problems or ongoing ransomware attacks, or perhaps your IT team has probed the client's employees with a phishing tool and they failed the test. The key is to identify a specific example of how your client's data was, or could be, compromised.



EXPLAINING THE VALUE OF SAT TO YOUR CLIENTS

STEP 2

Communicate the cost of SAT (and the cost of NOT using it)

Your clients will understandably want to know the required expenditure and potential ROI of an SAT program. Here are three questions you should be prepared to answer:

- ✓ How many of the client's employees would be enrolled in training?
- ✓ How much time would the client need to dedicate to training per year?
- ✓ What is the SAT seat license price you are offering?

And there are two questions your client must be able to answer:

- ✓ What is the hourly cost of those employees who will participate in training?
- ✓ If you've already been attacked, how much did it cost your company?

This last question is crucial, as the answer (when applied in Step 3) will often reveal that failing to employ SAT is actually more costly due to the financial damage inflicted by cyberattacks.



EXPLAINING THE VALUE OF SAT TO YOUR CLIENTS

STEP 3

Prove the SAT Program's ROI

Armed with the above information, you'll be able to calculate the projected ROI of an SAT program for your clients' specific businesses. The formula for this calculation is shown here:

$$\text{ROI}\% = \left(\frac{\text{savings}}{\text{cost}} - 1 \right) \times 100\%$$

Savings (from Preventing Cyberattack)

According to a 2017 UPS Capital study, the average cost of cyberattacks on SMBs ranges from \$84,000–\$148,000 (and that figure has very likely risen substantially since then). The actual savings figure your client would achieve by preventing a cyberattack is what you should plug into the above formula.

Other key factors to consider when assessing such savings:

- Loss of business revenue
- Damaged brand reputation

Cost (of Deploying SAT Program)

To find the cost of deploying an SAT program, use this simple equation:

Cost = program + time allocation

Where program cost = users x price per seat license

And time allocation = 4* hours per year x \$25* per hour x number of users

(*sample figures for illustrative purposes, actual figures may vary)



EXPLAINING THE VALUE OF SAT TO YOUR CLIENTS

STEP 4

Shift Thinking from IT-Centric to Company-Wide Security

As a matter of basic human nature, it's often difficult for people to effectively address a problem they don't completely understand.

To help your clients fully grasp the benefits of an SAT program, it's important that you shift their thinking from regarding cybersecurity as an IT problem to treating cybersecurity as a company-wide priority.

To that end, explain to your clients that hackers will look for the easiest way to get into their systems—and that path is often through the clients' employees. By receiving security awareness training, those employees will become far more aware of threats, and be more empowered to protect their organization.

You must shift the thinking **from...**

cybersecurity
is **ITs problem**

to...

cybersecurity
is a
**company
priority**



About VIPRE

VIPRE is a leading provider of internet security solutions purpose-built to protect businesses, solution providers, and home users from costly and malicious cyber threats. With over twenty years of industry expertise, VIPRE has one of the largest threat intelligence clouds, delivering unmatched protection against today's most aggressive online threats. Our award-winning portfolio of protection includes comprehensive endpoint, email, user and network security with threat intelligence for real-time malware analysis. VIPRE solutions deliver easy-to-use, comprehensive layered defense through cloud-based and server security, with mobile interfaces that enable instant threat response. VIPRE, a subsidiary of J2 Global, Inc., is headquartered in Florida and operates globally across North America and Europe.



www.VIPRE.com