How to

Prove ROI

of Security Awareness Training to Clients

Clients don't want raw numbers. They want reassurance that their risk is going down, their staff are improving, and their business is less likely to suffer downtime, fraud, or a costly breach.

This guide will show you how to:

- Measure the right SAT metrics
- Translate technical data into business outcomes
- Demonstrate compliance and insurance value
- Build client trust through reporting
- Create quarterly reports clients actually understand

Click a section to skip ahead.

PHIN

Why does SAT matter?

Most employees are already facing social engineering attacks far more often than they realize. Even when people understand cybersecurity best practices, those **habits fade without regular reminders, relevant examples, and practical reinforcement.**

of breaches involve the human element

2025 Verizon DBIR

Effective training helps organizations:

- Reduce risky behavior
- Improve security culture
- Meet cyber insurance & compliance requirements
- Reduce the likelihood of business interruption
- Protect sensitive data and finances

The Biggest Mistake When Reporting SAT Results

Many MSPs accidentally overwhelm clients with data while **failing to communicate outcomes.**

Clients do not care about:

- Endless dashboards
- Technical jargon
- Complicated risk scoring
- Twenty-page reports no one reads

Clients do care about:

- “Are we safer than before?”
- “Are employees improving?”
- “Are we reducing risk?”
- “Will this help us with compliance and insurance?”
- “Is this preventing downtime and fraud?”

How to prove ROI of SAT

To prove the value of SAT effectively, MSPs need to focus on three things:

Measuring the right metrics

Comparing them against a baseline

Translating results into plain English

That is how you turn SAT from a background service into something clients actively value.

Establish a Baseline

Behavior change takes time. One short training video is not going to transform an organization overnight, but consistent training over several months absolutely can. **Benchmarks help MSPs show measurable progress over time**. Without them, improvement becomes subjective.

With benchmarks, clients can clearly see that security awareness training is actually making a difference:

- Reduced phishing susceptibility
- Better reporting habits
- Improved training participation
- Stronger security culture

The longer you track trends, the easier it becomes to demonstrate value.
So, what should you be measuring?

The Most Important SAT Metrics to Measure

Not every metric matters equally. These are the **core KPIs** that consistently resonate with clients, along with **how to discuss them.**

Phishing Click Rate

This is still **one of the strongest indicators** of organizational risk. If phishing click rates decrease, risk decreases. If click rates rise, it signals a need for additional support or targeted coaching.

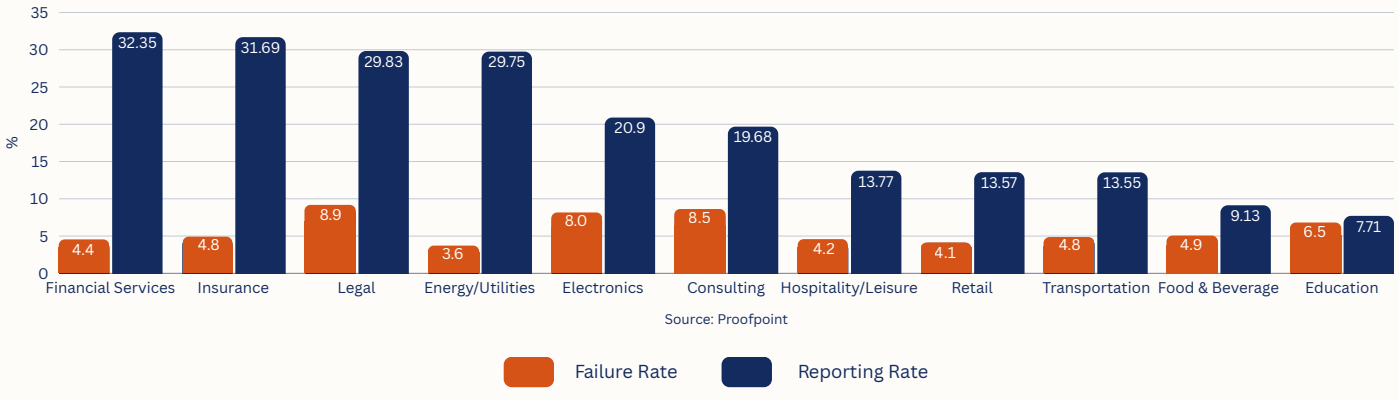
Many organizations average between **5% and 10% click rates** depending on industry and company size.
The closer to zero, the better.

What Clients Need to Hear

Don't say:
"Your phishing click rate decreased by 4%."

Try this instead:
"Your employees are becoming significantly less likely to fall for phishing attacks."

Industry Benchmarks
Phishing Simulation Failure Rate vs Reporting Rate



Source: Proofpoint

Return to top

Reporting Rate

Reporting rate measures how many employees actively identify and report suspicious emails.

A growing reporting rate usually means employees are becoming more confident and engaged. **This is important because early reporting helps stop attacks before they spread.**

What Clients Need to Hear

Don't say:
"Reporting rates increased by 12%."

Try this instead:
"Your team is identifying threats, helping prevent larger security issues."

Training Completion Rate

Training completion demonstrates participation and supports compliance requirements.

Users who repeatedly avoid training often become the highest-risk group inside the organization. This metric also matters for:

- Cyber insurance requirements
- Regulatory audits
- Internal policy compliance

What Clients Need to Hear

Don't say:
"Training completion reached 98%."

Try this instead:
"Your organization is meeting the training standards required for compliance and insurance readiness."

High-Risk Users

Every organization has **users who require additional attention.** These might include:

- Frequent phishing clickers
- Employees with privileged access
- Users who repeatedly skip training
- Employees handling sensitive financial data

Identifying high-risk users early helps reduce overall organizational exposure.

What Clients Need to Hear

Don't say:
"Three users remain high risk."

Try this instead:
"We identified a small group that needs additional support to reduce potential security risks. We recommend implementing the following steps to improve engagement."

Time to Complete Training

Employees are far more likely to engage with training when it is:

- **Short**
- **Relevant**
- **Easy to complete**
- **Practical**

Tracking training completion speed helps MSPs **demonstrate quality and efficiency.**

What Clients Need to Hear

Don't say:
"Training completion reached 98%."

Try this instead:
"The time spent completing training is significantly lower than the time and cost required to recover from a breach."

$4.4M

Average cost of a data breach globally.

IBM 2025 cost of a data breach report

Translating Technical Metrics Into Business Outcomes

Clients rarely care about cybersecurity metrics themselves. They care about what those metrics protect them from. **When discussing SAT results, focus on outcomes like:**

- Reduced risk of business interruption
- Lower chance of fraud
- Protection of critical accounts
- Stronger employee safety and confidence
- Compliant with insurance and industry regulations

The goal is to connect every technical improvement to a business benefit.

Know What SMBs Care About

- Fewer chances of business disruption
- Keeping a great reputation among clients
- Avoiding compliance fines and losing insurance coverage
- Fewer panic tickets and mistaken reports

Sell Outcomes

- Focus on risk reduction
- Highlight visible improvements
- Position training as a strategic part of a security plan
- Reinforce audit readiness and insurance benefits

Technical accuracy matters, but simplicity wins. **Avoid unnecessary cybersecurity jargon whenever possible.** Think about how professionals explain complex topics in other industries.

A doctor rarely says: (If they do, get a new doctor.)

You have acute erythematous dermal irritation.

They say:

You have a rash.

Your clients want that same clarity.

Instead of overwhelming them with cybersecurity terminology, explain:

1. What the issue is
2. Why it matters (to *them*)
3. What you are doing to improve it

Return to top

Demonstrating Compliance and Insurance Value

Many businesses adopt SAT because they feel required to. Insurance providers increasingly expect security awareness programs and compliance frameworks often require documented training.

That means reporting is not just about risk reduction — it's also about proving organizational readiness.

MSPs should regularly explain:

- Whether training participation meets compliance expectations
- Whether phishing performance supports cyber insurance requirements
- Whether any gaps could impact audits or renewals

Sometimes a single sentence confirming continued compliance is enough to justify the entire program in a client's eyes. But MSPs who **go beyond compliance** and demonstrate measurable business improvement **create even stronger client relationships.**

Building a Quarterly SAT Summary Clients Will Actually Read

The best SAT reports are:

- Short
- Visual
- Easy to understand
- Easy to share internally

In most cases, a single page is enough. Clients don't want lengthy cybersecurity dissertations. **They want quick clarity.**

Sample QBR SAT Report

During Q1 2026, **you have decreased the likelihood of getting breached by a phishing email,** with your phishing click rate dropping from 8.2% in month 1 to 3.6% in month 3.

94% of your employees have completed all of their trainings. You need 100% completion for cyber insurance. **We recommend taking the following actions to reach full completion...**

The following users are most likely to click a phishing email:

- User 1, Click rate
- User 2, Click rate

Here's what you should do to reduce their risk...

What to Include in a Quarterly SAT Summary

A Two-Sentence Executive Summary

This is often the most important part of the report and quickly communicates outcomes.

Example: "Your organization is now 22% less likely to experience a phishing-related security incident compared to last quarter. Training participation improved significantly, especially among previously high-risk users."

A Real-World Security Scenario

Help clients connect SAT to actual business protection. This creates emotional relevance. Clients remember stories far more than statistics.

Example: "This quarter, employees successfully identified and reported three phishing attempts that could have resulted in credential theft."

Three to Five Key Metrics

Refer to metrics →

Show progress over time. Quarter-over-quarter comparisons work well, especially when shown visually. These should also stay focused. Too many metrics dilutes the message.

When identifying high-risk users, **keep it constructive and solution-oriented**. The goal is improvement, not embarrassment.

The Long-Term Value of Clear SAT Reporting

When MSPs consistently report SAT outcomes clearly...

Security awareness training stops feeling like:

- A hassle
- A compliance checkbox
- Another wasteful invoice

Instead, clients begin to view it as:

A meaningful, measurable, and necessary business protection strategy.

Clear reporting strengthens:

- Client trust
- Retention
- Long-term partnerships
- Perceived MSP value

Want to make SAT reporting easier?

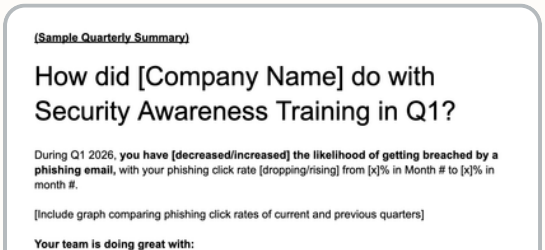
Build a **repeatable quarterly reporting process** that focuses on:

- Clear KPIs
- Business outcomes
- Compliance readiness
- Real-world impact

The **simpler and more understandable** your reporting becomes, the more your clients will realize the value of SAT.

Improve your reporting with this sample QBR template:

Download now


(Sample Quarterly Summary)

How did [Company Name] do with Security Awareness Training in Q1?

During Q1 2026, **you have [decreased/increased] the likelihood of getting breached by a phishing email,** with your phishing click rate [dropping/rising] from [x]% in Month # to [x]% in month #.

[Include graph comparing phishing click rates of current and previous quarters]

Your team is doing great with: