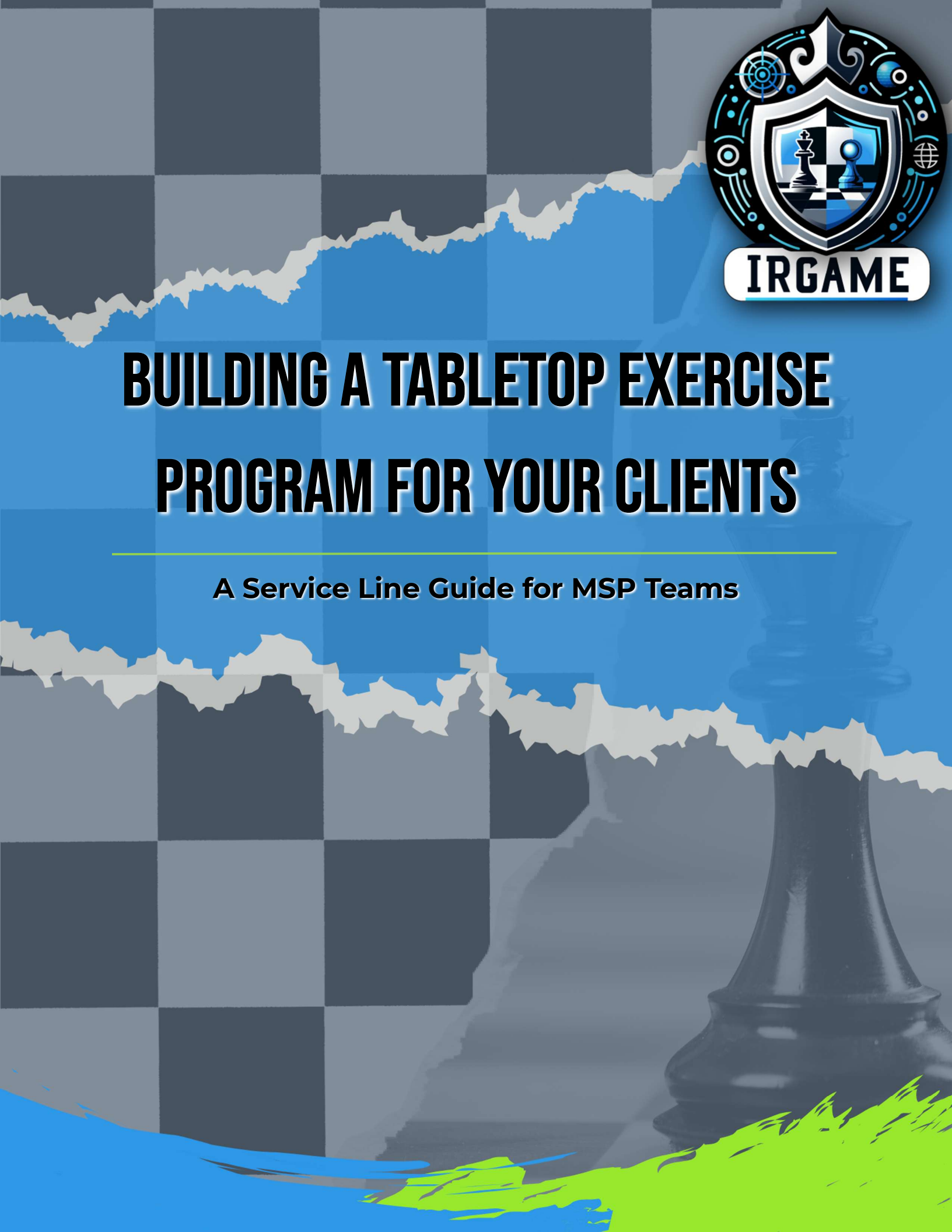


# BUILDING A TABLETOP EXERCISE PROGRAM FOR YOUR CLIENTS

A Service Line Guide for MSP Teams

# The Problem No One Is Talking About

**Five million-plus small and mid-sized businesses in the United States carry cyber insurance.** They pay premiums ranging from thousands to tens of thousands of dollars annually, and **the vast majority of them have never practiced responding to the incident they are insuring against.**

Think about what that means in practical terms. A business email compromise attack hits. The CEO has never made the call about what needs to happen and in what order. The CFO does not know what the policy covers or who to contact. The IT lead has never tested whether the backups restore in a useful timeframe. Everyone knows the plan exists, but no one has run it.

**This is the gap tabletop exercises close.** A tabletop is a facilitated, scenario-based discussion that walks an organization's leadership through a realistic cyber incident. No systems are touched. No live environment is at risk. Participants simply practice the decisions, communications, and coordination that a real incident demands.

The exercise format has been the standard preparedness methodology for government agencies, large enterprises, and healthcare systems for years. What is new is the accessibility, and that is where MSPs come in.

# What a Program Looks Like in Practice

**A tabletop exercise program is not a one-time event.** It is a recurring service delivered on a defined cadence, typically quarterly for clients with active compliance obligations, and annually at minimum for everyone else.

## THE EXERCISE ITSELF

A standard exercise runs approximately 90 minutes and follows a structured scenario. Common scenarios include ransomware, business email compromise (BEC), vendor supply chain compromise, AI compromise, and data exfiltration. The facilitator, typically someone on your team, presents a realistic incident in stages and asks participants to talk through their response decisions at each step.

Participants should include the client's decision-makers: the CEO, CFO, operations lead, and relevant IT personnel. The goal is not to test technical knowledge. It is to surface how the organization makes decisions under pressure and where the coordination breaks down.

## WHAT COMES OUT OF IT

Every exercise will allow you to produce a findings report that documents the gaps identified during the discussion. And there will be gaps. These are not hypothetical vulnerabilities. They are real organizational gaps: an IR plan that has not been updated in

two years, a cyber insurance policy no one can locate or worse, is stored on the network, a backup recovery process that has never been validated, a breach notification workflow that skips the legal team.

The findings report does three things. First, it creates a prioritized action plan the client can act on immediately. Second, it creates compliance documentation that cyber insurance carriers, regulators, and auditors increasingly require as proof that the organization has tested its response capabilities. Third, it establishes you as a strategic partner committed to helping the organization fix the gaps to reduce risk. This is a risk reduction service.

## THE ONBOARDING APPLICATION

A growing number of MSPs are now using tabletop exercises as part of the new client onboarding process, and the results have been significant.

During initial assessment of a prospective client, running a short tabletop scenario provides a window into how that organization functions under pressure. It reveals the maturity of the leadership team, the quality of existing documentation, the clarity of decision-making authority, and the degree to which IT and business leadership are aligned.

In practical terms: an MSP taking on a new client is making a risk decision. A client that cannot coordinate a response during a 90-minute exercise, has no documented IR plan, and has never discussed authority internally is a materially higher-risk engagement than one that has. The tabletop surfaces that risk up front, not after the first incident.

Some MSPs use it as a part of an onboarding fee that is an leadership assessment alongside a business risk, network, and hardware assessment, which establishes the service relationship and generates immediate revenue. Others include it as part of a more comprehensive onboarding audit. Either way, the exercise reframes how the prospective client sees the MSP: not as a vendor pitching services, but as a partner helping them understand their own preparedness and how to reduce their risk.

### WHAT MSPS ARE SEEING IN THE FIELD

MSPs who have added tabletops to their client onboarding report two consistent outcomes: they close more project deals because the exercise demonstrates value, and they lose fewer clients to competitors because the relationship is established at the strategic level from day one.

# Why Annual Exercises Are a Minimum, Not a Best, Practice

**The framing around tabletop exercises has shifted**. For years, the case was made on best practice grounds: forward-thinking organizations conduct exercises because preparedness reduces breach impact. That framing still holds. But it is no longer the primary reason clients should be doing this annually.

The primary reason is that multiple regulatory frameworks and the cyber insurance market now require documented evidence that organizations have tested their incident response plans. The question has moved from whether to do it to how to document it.  This is a risk discussion with the customer.  This is a risk discussion with the customer about how much exposure their leadership is willing to accept.

## PCI-DSS 4.0

The Payment Card Industry Data Security Standard version 4.0, which became the sole active standard in March 2025, includes an explicit annual testing requirement under Requirement 12.10.4. The previous version recommended testing but did not mandate it. The current version does. Organizations that accept credit card payments and are subject to PCI-DSS compliance cannot pass a QSA assessment without documented evidence of annual incident response testing. If the organization is just checking boxes and not actually testing their IR plan, their claims are almost guaranteed to be denied.

## HIPAA SECURITY RULE

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule has long required covered entities and business associates to implement an incident response plan under § 164.308(a)(6). What has changed is Office for Civil Rights (OCR) enforcement posture. Resolution agreements from 2024 enforcement actions now routinely include language requiring organizations to conduct tabletop exercises at least annually and submit documentation to OCR as a condition of the settlement. OCR has explicitly cited failure to test IR plans as an aggravating factor in penalty calculations.

## GLBA SAFEGUARDS RULE

The FTC's updated Gramm-Leach-Bliley Act Safeguards Rule, which took effect in 2023, requires financial institutions to implement and test incident response programs as part of their written information security program. This applies to a wide range of organizations beyond traditional banks, including mortgage brokers, auto dealers, tax preparers, and financial advisors.

### CMMC

The Cybersecurity Maturity Model Certification program, which governs defense contractor access to controlled unclassified information, includes incident response as a practice domain at Level 2 and above. Organizations seeking CMMC certification are expected to demonstrate that IR capabilities have been tested, not just documented.

| Framework | Testing Requirement |
|---|---|
| PCI-DSS 4.0 (Req. 12.10.4) | Annual testing — explicitly required as of March 2025 |
| HIPAA Security Rule (§ 164.308(a)(6)) | IR plan testing expected by OCR; required in enforcement settlements |
| GLBA Safeguards Rule (2023) | IR program testing required for covered financial institutions |
| CMMC Level 2+ | IR capabilities must be demonstrated, not just documented |

## The Cyber Insurance Dimension

**Cyber insurance underwriting has changed substantially** since the claims surge of 2021 through 2023. Carriers responded by tightening underwriting requirements, increasing scrutiny at renewal, and beginning to price risk based on demonstrated preparedness rather than policy declarations alone.

The current state of the market: major carriers are asking, upon application and at renewal, when the organization last tested its incident response plan, and are also asking for documentation. Organizations that cannot answer that question are seeing premium increases of 15 to 25 percent or sub-limits on certain cyber coverage. Organizations that can provide recent exercise documentation are qualifying for premium credits in the range of 5 to 15 percent.

The more significant risk is on the claims side. When an organization files a claim after an incident, the insurer's investigation examines what reasonable security measures were in place. An IR plan that was created and never tested is increasingly being treated as inadequate preparation, which some carriers have used as grounds to reduce claim payments. The exercise documentation is not just a compliance artifact. It is claim protection.

### THE MATH IS SIMPLE

A mid-market client paying $12,000 annually in cyber insurance premiums who can demonstrate annual tabletop exercise documentation may qualify for a 10% premium reduction, $1,200 per year, which offsets a significant portion of the exercise cost. The more important figure is the exposure: an untested IR plan creates grounds for claim reduction on a $250,000 ransomware settlement. One avoided claim reduction pays for exercises for a decade.

## The Financial Case for the Client

The ROI conversation for tabletop exercises is straightforward once the numbers are laid out.

According to IBM's 2024 Cost of a Data Breach Report, the global average cost of a data breach reached $4.88 million. For small and mid-sized organizations, the figures are lower but still substantial: average breach costs for organizations under 500 employees are in the range of $3 million to $4 million when full business impact is included. Organizations with a tested and documented incident response plan contained breaches approximately 54 days faster than those without, and faster containment directly correlates with lower total cost.

IBM's research also found that organizations with practiced response plans reduced breach costs by approximately 35 percent compared to those without. Applied to even a $500,000 small business breach scenario, that represents $175,000 in avoided costs on a single incident. The annual cost of a tabletop exercise program is a rounding error by comparison.

The conversation with a client should lead with the insurance and compliance case, because those are requirements. The ROI case reinforces the decision but rarely needs to close it on its own.

## The Three-Year Trajectory: From Optional to Required

**The market is moving in one direction.** Tabletop exercises are transitioning from a forward-thinking security practice to a documented requirement across the business landscape.

The 2025 to 2027 window matters for two reasons. First, the regulatory requirements now in effect, specifically PCI-DSS 4.0, the updated GLBA Safeguards Rule, and OCR's HIPAA

enforcement posture, create immediate demand that exists right now in your client base. Second, the window to establish this as a differentiated service is closing as more MSPs add it to their portfolio.

By 2027, analysts and practitioners tracking the regulatory landscape expect tabletop exercises to be a standard underwriting requirement across the cyber insurance market, not limited to large accounts or specific verticals. State-level regulations are already adding incident response testing language in California, New York, and others. Federal legislation requiring testing is in active discussion.

MSPs who have delivered 20 or 30 exercises will have established credibility, have developed facilitation skills, and built client relationships at the executive level that are very difficult for a competitor to displace. MSPs who begin offering the service in 2027 will enter a market where multiple competitors are already established and competing primarily on price.

## What This Means for Your Team

The practical question for anyone reading this document is: **How does a tabletop exercise program get built and delivered effectively?**

The facilitation role does not require deep technical expertise. It requires the ability to ask good questions, keep a structured discussion moving, and help participants discover gaps rather than lecturing them about gaps. That is a different skill set, and it is one that can be learned. The most effective facilitators are often not the most technical people in the room. They are the ones who can hold the strategic frame and keep the CEO and CFO engaged in the conversation.

The scenario content is the foundation of the service. Scenarios need to be realistic enough to surface genuine decision points, specific enough to the client's industry and size to feel credible and structured enough to be delivered consistently across different facilitators. Building that scenario library from scratch is a significant investment. Purpose-built platforms designed for MSP delivery handle that infrastructure, so your team focuses on facilitation and client relationships rather than content development.

The program structure that works for most MSPs is to start with existing clients where C-suite relationships already exist, deliver a small number of pilot exercises to build confidence and collect testimonials, and then expand outward to the broader client base and prospective clients using the compliance and insurance case as the lead message.

### BUILDING THE PROGRAM

At minimum, you need: a scenario library, a facilitation guide, a post-exercise report template, and a pricing structure. The service can be delivered remotely or on-site. Most exercises run for 90 minutes. Preparation per exercise, once a facilitator is trained, is typically 30 minutes or less.

Pricing in the current market for SMB clients ranges from $3,000 to $6,000 per exercise depending on client size, scenario complexity, and the depth of the findings report. Annual programs with multiple exercises can be priced at a volume discount that still generates substantial revenue while making the commitment easier for clients to accept.

The downstream effect is the more significant business case for the MSP. Every exercise identifies gaps. Many of those gaps represent implementation work: updating backup configurations, deploying better endpoint detection, revising documentation, adding security tooling. That work comes to your team. MSPs running regular tabletop programs consistently report that attributed project revenue exceeds direct exercise revenue within the first year.

#### THE STRATEGIC PARTNER POSITION

An MSP that facilitates tabletop exercises for a client's CEO and CFO is no longer competing on price with other MSPs who are not in that room. The relationship has shifted. The client is not thinking about switching providers because the MSP is now a trusted advisor on the business risk that matters most. What happens when something goes wrong. That is a position no SLA or service catalog creates on its own.

## How IRGame Makes This Program Operational

**IRGame is a tabletop exercise platform built specifically for the MSP channel.** It was created by the MSP operator community who experienced firsthand the gap between what enterprise incident response training looked like and what SMB clients could access and afford. The platform is designed to solve the four problems that prevent most MSPs from launching a tabletop program: scenario development, facilitation confidence, compliance documentation, and price accessibility.

### ONLINE, MULTIPLAYER, AND GEOGRAPHICALLY INDEPENDENT

IRGame is a web-based multiplayer platform. Every participant, whether the CEO sitting across the conference table or the CFO dialing in from another city, has their own browser-

based interface into the exercise. The facilitator runs the session from the same interface, advancing the scenario, deploying injects, and managing the discussion in real time.

This architecture means delivery is not constrained by location. An MSP can run the same exercise for a client whose leadership team is spread across multiple offices or facilitate an in-person session where everyone is in the room. The experience is the same either way: each participant sees the scenario unfold from their own perspective, which increases engagement and mirrors the information asymmetry that exists during a real incident.

For MSPs, this eliminates travel costs and scheduling friction entirely. You can deliver an exercise for a client across the country with no logistics overhead. For clients, it removes the barrier of getting a leadership team in the same room on the same day, which is often what prevents exercises from happening at all.

### NO CONFERENCE ROOM REQUIRED

Because IRGame runs in any web browser, a client's CEO can participate from their home office, the CFO from a client site, and the IT lead from headquarters all in the same exercise, simultaneously. The facilitator manages the session from wherever they are. Geography is not a factor.

## THE SCENARIO LIBRARY

IRGame's scenarios are structured, dynamic simulations built around the most common and high-impact incident types facing SMB clients: ransomware, business email compromise, supply chain compromise, third-party compromise, data exfiltration, AI compromise, and others. Each scenario is designed to run in 90 minutes and is structured in stages that mirror how a real incident unfolds.

The IRGame format is not a static slideshow. It is a dynamic dialog-based simulation that presents realistic decision points in sequence, adjusting the pressure of the scenario as the exercise progresses. Participants are forced to make decisions with incomplete information under time pressure, which is exactly what a real incident demands. The format is engaging enough that C-suite participants, who typically resist being lectured at in security briefings, stay active throughout the exercise.

Each scenario includes a facilitator guide with suggested questions, discussion prompts, and injects that deepen the exercise. This means an MSP team member who has never run a tabletop before can deliver a professional, credible exercise within days of onboarding, not months.

## WHAT THE PLATFORM PROVIDES THE FACILITATOR

IRGame handles the infrastructure that would otherwise take an MSP hundreds of hours to build independently. The scenario library is developed and maintained by incident response professionals and updated as the threat landscape evolves. The facilitation guides provide structure without scripting the facilitator into a corner. The platform is designed so that the MSP's team member is the expert in the room, not a reader of someone else's content.

Specific capabilities the platform provides:

- A library of scenarios covering the primary incident types relevant to SMB clients across industries
- Facilitator guides with stage-by-stage discussion questions designed to surface organizational gaps rather than test technical knowledge
- Post-exercise findings report templates that produce compliance-ready documentation meeting the standards required by an increasing number of cyber insurance carriers
- Facilitator training designed to get an MSP team member from zero experience to delivering a credible first exercise in a short onboarding period
- A browser-based multiplayer interface that supports both fully remote and in-person delivery without additional setup or tooling

## COMPLIANCE DOCUMENTATION BUILT IN

One of the highest-value outputs of a tabletop exercise is the paper trail it creates. Regulators, auditors, and insurance underwriters do not accept verbal confirmation that an exercise occurred. They need dated documentation, participant records, scenario descriptions, findings, and remediation action plans.

IRGame's post-exercise reporting structure is built around those requirements. The “Day After” report generated for each exercise is formatted to satisfy the documentation expectations of audit standards for cyber insurance carrier requests. The MSP delivers the exercise, adds their insights to the report, and the client walks away with a document they can hand to an auditor or underwriter.

This documentation capability is not an afterthought. It is a core part of the value proposition. Clients are paying for preparedness and for proof of preparedness. IRGame ensures the MSP can deliver both in a single engagement.

## THE ONBOARDING-TO-PROGRAM PIPELINE

IRGame's scenario library includes exercises designed for initial client assessment as well as ongoing program delivery. For MSPs using tabletops as an onboarding tool, the platform provides a structured exercise format that works as a diagnostic: it is professional enough to establish credibility, focused enough to reveal decision-making quality, and short enough to fit within an initial assessment engagement.

For ongoing program clients, the scenario library provides enough breadth to run a different scenario at each quarterly exercise without repetition. Clients who go through a ransomware scenario in Q1, a BEC scenario in Q2, a supply chain compromise in Q3, and a data exfiltration scenario in Q4 are building genuine muscle memory across the full range of incident types, not just checking a single compliance box.

## THE MSP BUSINESS MODEL

IRGame operates on a partner model designed for the MSP channel. The platform is subscription-based at the MSP level, with a small monthly subscription fee. Once subscribed, you can deliver exercises with as many clients as your team can schedule and pay a per game fee for use.

The pricing structure is designed so that a single exercise at market rates pays for the platform subscription multiple times over. MSPs delivering 20 or more exercises annually typically see platform costs represent a small percentage of total exercise revenue.

IRGame also provides marketing support materials that MSPs can use under their own brand, including service descriptions, client-facing one-pagers, and outreach templates. The intent is for the client to see your MSP as the provider of this service, with IRGame functioning as the back-end infrastructure. The relationship belongs to you.

### BUILT FOR THE MSP CHANNEL

IRGame was not adapted from an enterprise product and scaled down. It was designed from the start by MSPs for the MSP delivery model: recurring client relationships, SMB-scale organizations, and a team that needs to deliver professional exercises without a dedicated security consulting practice. The platform reflects that design in every element, from scenario length to report format to facilitator training.

# The Revenue Opportunity: A Simple Business Model

The average MSP carries approximately 60 clients. At a 25 percent Year 1 adoption rate, that is 15 clients running one exercise each. The numbers from that starting point are worth laying out explicitly, because **the direct exercise revenue is only part of the story.**

## YEAR 1 BASELINE: 15 CLIENTS, ONE EXERCISE EACH

Example exercise price: $3,500 per engagement (suggested minimum), supporting up to 14 participants (two tables of seven, which is the standard IRGame session structure). Preparation time per exercise, once a facilitator is trained, is approximately 30 minutes. Delivery is 90 minutes. Total time investment per exercise is roughly two hours, not counting the findings report.

| Revenue Stream | How It Calculates | Year 1 Total |
|---|---|---|
| Direct exercise revenue | 15 clients × $3,500 | $52,500 |
| Attributed project revenue (approx.) | $52,500 × 2x | $105,000 |
| **Combined Year 1 impact** | **15 exercises + projects** | **$157,500** |

The costs for providing this service are a fraction of the revenue stream. Providing this service should provide between 70 and 80% gross margins. Remember that the average SMB tabletop costs $10,000.00+. You will be able to get the mentioned gross margins and still provide a service that is half or more less expensive than traditional TTX methods.

## WHAT THE PROJECT REVENUE REPRESENTS

The 2x project multiplier is not a theoretical figure. It reflects the consistent pattern MSPs see after delivering exercises: every findings report surfaces gaps, and gaps represent work. The types of projects that regularly emerge from tabletop exercises include IR plan development or updates, backup and recovery validation and remediation, endpoint detection and response deployment or upgrades, AI readiness, cyber insurance policy reviews, breach notification procedure documentation, and employee security awareness programs.

These are not manufactured upsells. They are legitimate deficiencies the client discovered during the exercise. The MSP did not identify them through an audit and pitch a fix. The client identified them by living through a simulated incident and recognizing that they were not prepared. That is a very different conversation, and it closes at a very different rate.

## WHAT GROWTH LOOKS LIKE BEYOND YEAR 1

The Year 1 model uses 25 percent adoption because that is a realistic number for a program that is new to the market and the client base. Year 2 changes the math in two ways. First, the 15 clients from Year 1 are now annual renewals, not new sales. Second, the remaining 45 clients are now prospects with context: they have heard about the program from peers, they have seen the compliance and insurance requirements tighten, and some of them are now being asked for exercise documentation at renewal.

A conservative Year 2 assumption adds another 15 clients to the program while renewing the original 15, bringing the active client count to 30. Direct exercise revenue doubles to $105,000. Attributed project revenue, now drawing from a larger and more mature client base, scales proportionally. The program that generated $157,500 in Year 1 is on a path to $315,000 or more in Year 2 without adding a single new client to the MSP's roster.

### THE COMPOUNDING EFFECT

Tabletop exercise programs grow on two axes simultaneously: more clients adopting the service each year, and existing clients moving from annual to quarterly exercises as compliance requirements tighten. An MSP at 50 percent client adoption running a mix of annual and quarterly programs is not looking at the Year 1 numbers above. They are looking at a multiple of them.

## TIME INVESTMENT VS. REVENUE RETURN

At 15 exercises in Year 1, the facilitator time investment is approximately 30 hours: 30 minutes of preparation and 90 minutes of delivery per exercise, plus findings report generation. That is before accounting for IRGame's report templates, which substantially reduce documentation time. Against $157,500 in combined revenue, the time-to-revenue ratio is difficult to match with any other service line an MSP can add in a comparable timeframe.

The more relevant comparison is not hours per dollar. It is what those 15 exercises do to client relationships. Every exercise places your team in a room with the CEO and CFO in a context that no managed services agreement, no QBR, and no security assessment replicates. The exercise is where the strategic partnership is built, and the revenue that follows is a consequence of that relationship, not just a transaction.

The demand for this service exists today. Regulatory requirements are already in effect for clients in healthcare, financial services, and any business that accepts credit card payments. Cyber insurance underwriters are already asking for exercise documentation at renewal. The client relationships that benefit most from tabletop exercises are the ones you already have.

IRGame provides the platform infrastructure that makes the program operational without the multi-month build cycle. The scenario library, facilitation guides, compliance documentation framework, and facilitator training are in place. What the MSP contributes is the client relationship, the delivery context, and the downstream implementation capability when exercises reveal gaps that need to be addressed.

The MSPs who establish this practice in the current window will own the relationship position and the market reputation before the broader competitive field catches up. The ones who wait will build the same capability in a more crowded market, without the early-mover client relationships and without the testimonials and case studies that close deals.

The question is not whether your clients need this. They do. The question is whether you are the one who delivers it to them.

**CONSIDER THIS**

Adding as little as $100 per month per client is enough to cover the cost of running one exercise per year across your entire client base. At market rates, the price to the customer should be a minimum of $3,500 to $6,000. The lowest rate for a traditional tabletop exercise is $10,000, and that does not count the time people spend in a conference room looking at slides or the travel expense of bringing everyone into the office.

## Conclusion

**Tabletop exercises represent a practical and highly scalable opportunity for MSPs to move beyond reactive IT support and become strategic cybersecurity advisors to their clients.** By helping organizations rehearse incident response in a realistic but low-risk environment, MSPs can uncover operational gaps, strengthen executive decision-making, improve compliance readiness, and create meaningful recurring service revenue, all while delivering measurable client value.

As cyber insurance requirements tighten and regulatory expectations increase, preparedness is shifting from a “nice to have” to a business necessity. **MSPs that establish a structured tabletop exercise program now will be well positioned to differentiate in a crowded market, deepen client relationships at the leadership level, and build a defensible service line around resilience, not just remediation.**

# Sources and References


1. IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation. Retrieved from https://www.ibm.com/reports/data-breach
2. Payment Card Industry Security Standards Council. (2022). PCI DSS v4.0 — Requirement 12.10: Incident Response Plan. PCI SSC. Effective March 31, 2025. Retrieved from https://www.pcisecuritystandards.org
3. U.S. Department of Health and Human Services, Office for Civil Rights. (2023). HIPAA Security Rule: Incident Response — § 164.308(a)(6). HHS.gov. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
4. Federal Trade Commission. (2023). FTC Safeguards Rule (16 CFR Part 314) — Updated Requirements for Financial Institutions. FTC.gov. Retrieved from https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
5. U.S. Department of Defense. (2024). Cybersecurity Maturity Model Certification (CMMC) Program — 32 CFR Part 170. DoD. Retrieved from https://www.acq.osd.mil/cmmc
6. U.S. Department of Health and Human Services, Office for Civil Rights. (2024). HHS OCR Resolution Agreements and Corrective Action Plans. HHS.gov. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
7. IRGame, Inc. (2025). IRGame Platform — Tabletop Exercise Delivery for MSPs. Retrieved from https://www.irgame.ai
8. Marsh McLennan. (2024). The State of the Cyber Insurance Market. Marsh. Retrieved from https://www.marsh.com/us/insights/research/us-cyber-insurance-pricing.html
9. New York Department of Financial Services. (2023). 23 NYCRR 500 — Cybersecurity Requirements for Financial Services Companies. NYDFS. Retrieved from https://www.dfs.ny.gov/industry_guidance/cybersecurity