usecure

The Ultimate MSP Guide to Selling Human Risk Management

Proven plays, messaging frameworks, and real-world strategies to win deals, boost retention, and grow recurring revenue.

Table of contents

Introduction

A human risk management playbook

Traditional security awareness training falls short of today's cybersecurity demands. This playbook shares usecure's proven approach to help MSPs shift to full Human Risk Management (HRM) solutions that drive real results.

Based on our top-performing MSP partners, this guide helps you:

- Turn technical metrics into business value
- Position HRM as a strategic investment
- Overcome objections with tested tools
- Unlock recurring revenue through smart bundling

Get actionable insights, proven templates, and real-world examples to grow your security practice and better protect your clients.

> The biggest cybersecurity risk is people, not technology. Traditional training fails to change behavior, so MSPs must move beyond security awareness training to Human Risk Management.
>
> Embedding HRM boosts security, unlocks revenue, and strengthens client retention. This playbook guides you to real security outcomes and long-term growth.

Charles Preston
Founder and CEO, usecure

The $1 Trillion Opportunity: Why MSPs Must Lead the Shift to HRM

The cybersecurity landscape is shifting—and so are client expectations.

✓ Internal threats are rising.
✓ Compliance is more complex.
✓ Cyber insurance is more demanding.
✓ And most importantly: human error remains the #1 cause of breaches.

Yet most SMBs still rely on basic training platforms that stop at "awareness"—leaving them (and their MSPs) exposed.

Industry Snapshot

- Security awareness market: $10B by 2027
- Global MSP market: $1T+ by 2033
- 90% of breaches still involve human error

This is where modern MSPs are stepping in.

They’re moving beyond static training to offer strategic Human Risk Management (HRM)—solutions that continuously reduce human risk, boost compliance readiness, and deliver measurable business value.

And the best part? You don’t need to build it from scratch. This guide breaks down exactly how to position, pitch, and profit from HRM—starting today.

Market trends driving HRM adoption

AI threats require adaptive learning solutions like usecure's bite-sized training modules that evolve alongside emerging risks.

Evolving cyber threats

AI-driven phishing campaigns and advanced social engineering tactics have made human vulnerabilities a primary target. In 2024, 90% of cyberattacks involved social engineering, with phishing as the most common method (Verizon DBIR 2024).

Remote work and shadow IT

The rise of remote work has increased reliance on unauthorized shadow IT tools, creating security blind spots. 68% of employees use unsanctioned apps, exposing organizations to compliance and data security risks (Gartner, 2024).

Human error

Infosec Institute reports that 74% of cybersecurity incidents include a human element. This includes falling for phishing attacks, sharing credentials, or mishandling sensitive data (IBM Cyber Security Intelligence Index Report).

Compliance and cyber insurance

Stricter regulations like GDPR and ISO 27001 require robust risk management strategies. Additionally, cyber insurance premiums are projected to increase by 15% to 20% annually, reaching approximately $23 billion by 2026, up from an estimated $14 billion at the close of 2023. Insurers are increasingly demanding evidence of employee training and compliance measures.

Why Awareness Training Is Failing—and What MSPs Can Do Instead

The market is changing—and fast. While traditional security awareness training (SAT) has helped tick compliance boxes, it hasn't solved the actual problem: people are still making security mistakes.

As a result, clients are demanding more, and MSPs offering generic SAT are starting to lose ground.

Let's break it down:

The Awareness Trap: What No Longer Works

- Compliance-first training, but little behavioral change
- One-size-fits-all courses—regardless of role or risk
- Reports based on course completions, not actual risk reduction

The result?
Clients may pass audits, but they're still vulnerable—and they know it.

VS

New-school human risk management approach

- Aimed at building a security culture and driving secure behavior
- Engaging micro-training, tailored to each users unique risk areas
- Ongoing risk is calculated through multiple data points

MSP Tip:

"Awareness training" isn't a dirty word—it's just step one. What sells today is a strategic layer that turns user behavior into measurable security improvement.

From Awareness to Impact – HRM vs. Traditional SAT

Aspect	Traditional SAT	Human Risk Management
Focus	Training completion rates	Risk reduction and behavior change
Engagement	Generic, one-size-fits-all	Personalized, bite-sized training
Impact	Limited measurable outcomes	Reduced phishing susceptibility, improved compliance readiness
Scalability	Manual processes per client	Automated enrollment, training, and reporting

How HRM Drives Retention and Revenue Growth

HRM helps MSPs keep clients longer, increase contract value, and scale efficiently —without adding internal overhead.

- **Client Stickiness: Show real results—lower risk scores, fewer phishing clicks, improved compliance.**
- **Upsell Foundation: Build on HRM with breach monitoring, policy automation, or advanced reporting.**
- **Scalable Delivery: Automation lets you serve more clients without increasing workload.**

Pro Tip: Use HRM data to prove ROI, position it as a strategic service (not just training), and bundle it into a broader security offering.

usecure Case Study: How IT Visionaren Climbed Client Success with usecure's HRM platform

- Challenge: IT Visionaren needed to train hundreds of end users across multiple clients without overwhelming their small team with administrative tasks.
- Solution: By leveraging usecure's AutoEnrol and AutoPhish features, IT Visionaren automated training enrollment and phishing simulations, reducing manual effort while improving client security awareness.
- Result: Clients reported increased employee awareness of cyber threats, particularly phishing attacks, while IT Visionaren scaled their services with minimal admin overhead.
- Key Takeaway: Automation allowed IT Visionaren to protect client environments efficiently while focusing on business growth.

HRM's Impact on Client Retention & Revenue

- **Higher Retention: Clients renew when they see measurable security improvements, like reduced phishing risks and faster compliance.**
- **Upsell Potential: Bundle HRM with premium add-ons like dark web monitoring or advanced reporting to increase contract value.**
- **Scalable Growth: Automation minimizes admin work, allowing MSPs to expand services without adding resource costs.**

IT Visionaren Case Study →

How to sell HRM as a strategic security investment

> HRM is a strategic security layer that complements existing technical defenses like firewalls.
>
> By reducing human risk, HRM enhances an organization's resilience to threats and fosters a security-conscious workforce.

The Human Side of Risk Management

HRM places people at the center of security. It recognizes that human behavior—the decisions, mistakes, and instincts of employees—is a critical factor in cybersecurity. Just as we assess personal risks in daily life, businesses must understand and manage the human element of organizational risk.

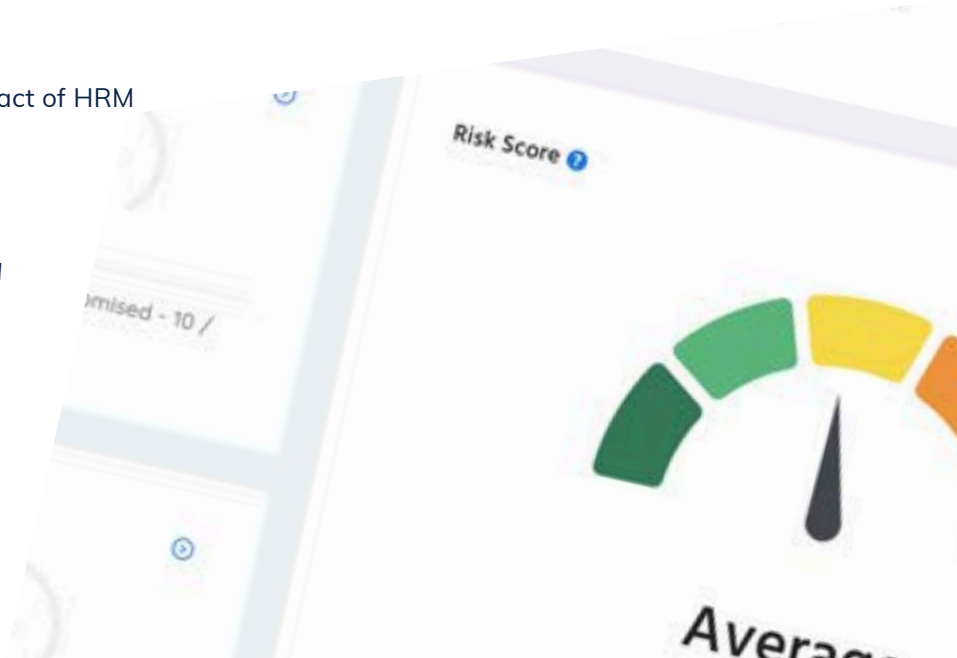
Human-Centered Risk Management: A Strategic Shift

- Identify and Address Human Risk: HRM automatically flags high-risk behaviors and delivers targeted interventions.
- Promote Continuous Learning: HRM ensures employees are consistently trained with adaptive, bite-sized content, evolving alongside emerging threats.
- Foster Empathy and Responsibility: By involving employees in security, HRM makes them an integral part of the solution.

ROI Storytelling: Positioning HRM as a Strategic Investment

Instead of focusing on training completion rates, MSPs should talk about the real-world impact of HRM—reduced risk and increased organizational resilience.
Here are ways to frame HRM's ROI:

- **Proactive Risk Reduction:**
  "Rather than simply completing training, HRM enables you to identify high-risk behaviors and target specific employees for tailored interventions. This leads to fewer security incidents."
- **Cost Avoidance:**
  "With HRM, your organization can avoid costly breaches, which average $4 million globally, addressing human risk before it materializes."
- **Improved Compliance:**
  "HRM makes it easier to comply with regulations like GDPR and ISO 27001 by reducing human errors, streamlining compliance workflows, and providing automated reporting."



Who are you selling to?

Before diving into how to package and sell usecure effectively, it's important to understand the key buyer personas MSPs typically encounter. Each persona has unique pain points, priorities, and decision-making criteria. Tailoring your pitch to these personas will help you close deals faster and build stronger client relationships.

IT Managers at SMBs

Challenge

- Overwhelmed by managing IT infrastructure with limited resources.
- Struggle to ensure employees follow security protocols.

Need

- Automated solutions that reduce manual effort and improve security outcomes.
- Tools that simplify compliance audits and reporting.

Business Owners / Executives

Challenge

- Concerned about financial loss or reputational damage from cyber incidents.
- Increasing pressure to meet cyber insurance or compliance requirements.

Need

- Clear ROI and measurable risk reduction to justify investment.
- Proactive solutions that protect their business without disrupting operations.

HR or Compliance Officers

Challenge

- Difficulty engaging employees in training programs.
- Struggle to track policy acknowledgments and ensure audit readiness.

Need

- User-friendly platforms that drive employee participation and simplify compliance.
- Automated tools for policy management and reporting.

How these personas align with packaging plans

- Core Plan: Ideal for IT Managers who need a quick, automated solution to improve employee awareness without adding complexity.
- Advanced Plan: Perfect for Business Owners or Compliance Officers who require tailored solutions with advanced features like policy management or custom phishing templates.

How to pitch HRM to different buyer personas

To close more deals, tailor your messaging to the stakeholder in front of you. Whether you're speaking to IT, leadership, or compliance, lead with the outcomes that matter most to them—efficiency, protection, compliance, and peace of mind.

Persona	Pain Points	How to Position HRM	Key Messaging Tips
IT Managers at SMBs	• Limited time/resources - Struggle with user compliance • Need automation & visibility	• Make their job easier with automation • Reduce workload with seamless integrations (Microsoft 365, Google Workspace) • Improve compliance without manual intervention	• "HRM automates training, policies, and reporting so you don't have to manually chase employees or track progress." • "You'll have a dashboard to see which employees pose the biggest security risks—without running manual audits."
Business Owners / Executives	• Financial risk from cyber incidents • Cyber insurance & compliance pressures • Worried about reputational damage	• Risk-based approach: usecure reduces liability and ensures regulatory compliance • Competitive advantage: A secure company builds customer trust	• "90% of breaches come from human error—HRM actively reduces risk, not just reports on it." • "Clients that prioritize HRM have lower insurance premiums and fewer security incidents."
HR / Compliance Officers	• Ensuring employees complete training • Tracking policy compliance • Audit readiness & reporting headaches	• Automated compliance management saves time • Instant reporting for audits & insurance • Better employee engagement with shorter, interactive training	• "Instead of chasing employees, HRM automates reminders and ensures full policy acknowledgment." • "You can instantly pull compliance reports for auditors—no more spreadsheets or manual tracking."

Before moving forward, make sure you've identified your ideal SMB clients. If you haven't, take a moment to define your target market using the buyer personas outlined above.

Action Step: Review the Buyer Personas section and write down your top 3 target SMB types.

Dive into our Go-to Market HRM Strategy for in-depth steps >

Involve Your Team in the Playbook Process

To make the most of this playbook, identify key team members within your MSP business who will champion its implementation. These individuals will ensure the content is actionable, delivered on time, and continuously refined to meet client needs.

For the best results, your playbook should be championed by leadership and adopted across all relevant roles in your MSP.

Who	How they influence the playbook	How the playbook influences them
MSP Business Owners / Leadership Team	- Serve as champions for HRM adoption. - Provide strategic direction for bundling and pricing.	- Drive revenue growth through HRM solutions. - Build a culture of proactive cybersecurity services.
Service Delivery Managers (SDMs)	- Define processes for onboarding and managing HRM deployments. - Provide insights into operational challenges.	- Streamline client onboarding and ongoing management tasks. - Improve efficiency with automation and policy management.
Account Managers / Client Success Managers	- Test, gather feedback, and refine sales approaches. - Keep HRM offerings dynamic and tailored to client needs.	- Strengthen client relationships through measurable outcomes. - Increase upsell opportunities with bundled solutions.
Technical Engineers / Security Specialists	- Provide technical expertise for deployment guides. - Ensure seamless integration with Microsoft 365/Google Workspace.	- Simplify deployment with pre-configured templates. - Automate routine tasks like user synchronization.
Sales Teams (BDRs/Account Executives)	- Use feedback from prospects to refine messaging.	- Close deals faster with objection-handling scripts and tools. - Clarify HRM's value proposition to clients effectively.

Discover How usecure Empowers MSPs to Deliver Results

Now that you understand the opportunity and strategy behind Human Risk Management, let's explore how usecure equips MSPs with the tools to put these insights into action. The following section breaks down the core features that help you automate, scale, and prove the value of HRM—enabling you to win new clients, drive recurring revenue, and stand out in a crowded market.

usecure's HRM Solution

See usecure's key features in action

Explore MSP Demo Hub

uLearn

Security awareness training

- Automated user training
- Custom course builder (LMS)
- User-tailored programs
- 100+ readily-made courses
- Ongoing training reporting

uPhish

Simulated phishing

- Automated phishing tests
- Custom template builder
- 700+ readily made templates
- End-user phish alert button
- Ongoing phishing reporting

uBreach

Dark web monitoring

- Dark web breach monitoring
- Identify exposed user accounts
- Locate the breached services
- Learn what data is exposed
- Dig down into user breaches

uPolicy

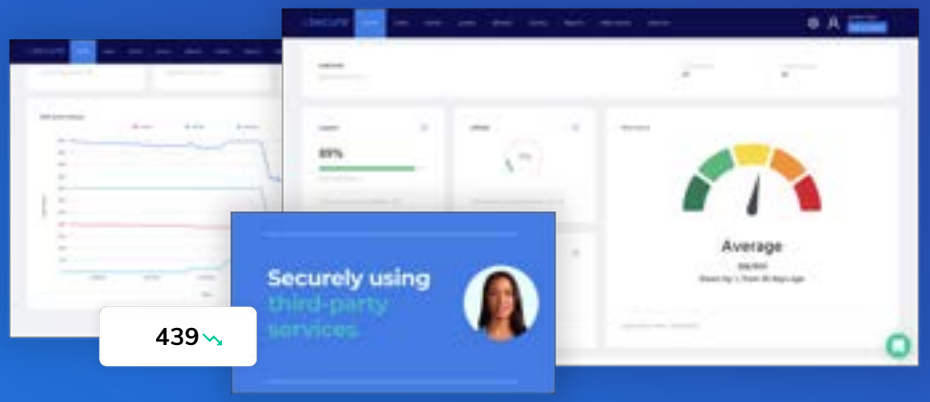
Policy management

- Automated policy approvals
- Centralized policy library
- Essential policy templates
- Edit and build custom policies
- Track outstanding signatures

Risk Reporting

Human Risk Analytics

- Company-wide human risk scoring
- uLearn, uPhish, uBreach and uPolicy performance
- Self-access employee risk profiles (End User Portal)
- Real-time reporting dashboard with key metrics
- Automated email summary reports for clients



The road to recurring revenue

Whether you're just introducing HRM or looking to grow existing accounts, this simple 5-step motion helps you close faster, prove value early, and retain clients longer.

Prospecting	Discovery Call	Human Risk Report		Free Trial	Convert to Paid
1	2	3	OR	3	4
Goal	**Goal**	**Goal**		**Goal**	**Goal**
Set discovery meeting	Identify risk and qualify the opportunity	Demonstrate risk		Demonstrate value	Start automatic billing
Actions	**Actions**	**Actions**		**Actions**	**Actions**
• Promote your human risk service via email, calls, or social. Hook with relevant trends and book a discovery meeting.	• Run discovery meeting, qualify lead, identify pains, demo the service, promote the HRR/trial.	• Enrol client on a HRR. generate the report, and present the results in a follow-up meeting.		• Use HRR findings to recommend action. Offer a trial or proceed directly to onboarding.	• Run follow-up call, discuss how investing in training now will reduce their existing risk.
Tip	**Tip**	**Tip**		**Tip**	**Tip**
• Lead with a stat or question: "90% of breaches start with people—how are you managing that risk today?"	• Use consultative questions to spotlight risk blind spots and security frustrations.	• Book the follow-up during the HRR setup. Use the data to drive urgency, not just interest.		• If risk is clear, skip the trial. Convert momentum into deployment while urgency is high.	• Frame the purchase around liability reduction and compliance simplicity—not just features.

Overcoming Common Sales Objections

"We already have a cybersecurity solution in place."

Counter with:

- Layered security approach: Technical defenses don't address human risk—90% of breaches involve human error.
- Complement, not replace: usecure strengthens existing security by reducing risky behaviors.

"We don't see enough value to justify the cost.."

Counter with:

- Cost of inaction: A single breach costs significantly more than proactive risk management.
- Clear ROI: Fewer incidents, lower cyber insurance premiums, and stronger compliance.

"We're too small for this."

Counter with:

- SMBs are prime targets: Hackers know smaller businesses lack dedicated security teams.
- Affordable & scalable: Tailored pricing ensures it fits businesses of all sizes.

"My staff members won't actually engage with a program?"

Counter with:

- MSP-exclusive benefits: Additional management, support, and strategic guidance that vendors don't offer.
- Fully managed service: Saves their internal team time while ensuring proper implementation.

"We've never had a security incident, so we don't need this."

Counter with:

- Security isn't about luck: Breaches happen without warning—prevention is cheaper than response.
- Compliance & insurance: Proactive HRM helps meet evolving security requirements.

"We tried this before, and it didn't work."

Counter with:

- What didn't work? Identify past issues and highlight how usecure solves them.
- Proven engagement: Personalized, bite-sized training drives better results.

Outreach: Connecting with the right prospects

Once we know who we want to sell to, it's time to reach out. A well-structured outreach strategy ensures you connect with the right prospects at the right time, increasing your chances of closing deals.

Example Sales Pitches

Email Pitch

Subject Line: Reduce Your Cyber Risk with One Simple Step Hi [First Name],

I noticed that [Company Name] operates in [Industry], where phishing and compliance risks are growing concerns.

We specialize in helping businesses like yours reduce human cyber risk through automated training, phishing simulations, and policy management.

Would you be open to a quick call? I'd love to share how our platform has helped businesses like [Case Study Example] reduce phishing risk by 90%.

Best regards, [Your Name]

Phone Script
"Hi [Prospect], this is [Your Name] from [Your MSP]. We help businesses reduce human cyber risk through proactive solutions that go beyond traditional training programs.

I'd love to schedule a quick call to show you how we've helped companies like yours improve security awareness while simplifying compliance."

"The key is to use a routine cadence—a combination of outreach tactics repeated systematically for each prospect. This approach ensures consistent follow-ups and keeps your message in front of potential buyers.

Nihil Morjaria
Chief Revenue Officer
at usecure

Maximizing the Impact of Human Risk Assessments

Running a Human Risk Report (HRR) is one of the most effective ways for MSPs to demonstrate value and accelerate the sales process. To get the most from every HRR:

Get an upfront contract

Doing this before running a HRR helps identify more worthwhile prospects who want to justify a purchase. “If we do find a lot of risk data, such as staff giving away a password during a phishing simulation, which actions would you want to take to mitigate those risks?”. You can then refer to this post-HRR.

Set expectations

Before launching the assessment, discuss with your prospect what they hope to learn from each stage, including breach scans and phishing simulations. Sharing examples from similar businesses can help clarify likely outcomes, such as discovering compromised credentials or users susceptible to phishing.

Agree on a timeframe

Agree on a clear timeframe for running the Human Risk Report and setting up phishing simulations. Use Message Injection to simplify setup by removing the need for allowlisting and speeding delivery. Emphasize how easy it is to get started quickly and begin gathering meaningful data without delay.

Use a targeted phish

Select a realistic phishing campaign that mirrors real-world threats to accurately assess your organization’s vulnerability to social engineering attacks.

Set up a follow-up call

Make sure to schedule a call for after the HRR is completed to discuss the risk results. Some MSPs have success when running a short call after the breach scan stage in order to review the data and confirm specifics on the phish. Some prospects, however, might just prefer having the pre-HRR and post-HRR calls.

Be transactional

In the post-HRR call, refer back to their expectations and upfront contract, e.g. “You mentioned that, if there’s a staff compromise, you would want to roll out training and regular phishes. We can get a program set up for you today for just $X per user, per month. Shall we get the training deployed today...?”.

The human-centered approach to compliance & cyber insurance

HRM isn't just another security layer—it's a strategic growth lever for MSPs. By tackling the human element of cybersecurity, MSPs can increase client retention, reduce compliance risk, and drive recurring revenue with services that align to modern buyer expectations.

Why Compliance & Cyber Insurance Require a Human Risk Strategy:

- Regulatory mandates (GDPR, HIPAA, ISO 27001) require organizations to manage human risk, making HRM essential for audits & liability reduction.
- Cyber insurers increasingly demand proactive security measures—lack of compliance can lead to denied claims or higher premiums.
- SMBs face growing pressure from partners & clients to demonstrate cybersecurity resilience.

How HRM Simplifies Compliance & Reduces Liability Risks

Automated Policy Management – Ensures security standards are met with audit-ready documentation.

Risk-Based Training & Reporting – Tailored programs address compliance needs while automated reports simplify audits.

Proactive Risk Mitigation – Features like phishing simulations & dark web monitoring prevent threats before they escalate.

Selling HRM Through Compliance & Insurance Trends

- Educate Prospects – Show financial & reputational risks of non-compliance.
- Demonstrate Value – Use Human Risk Reports (HRR) to highlight vulnerabilities.
- Position HRM as a Dual Solution – Compliance enabler & risk mitigator.
- Leverage ROI Storytelling – Show real-world success in reducing audit times, preventing fines & lowering premiums.

When you lead with human risk, you position your MSP as a trusted partner—not just another tool provider.

Follow up templates

Post-Discovery Call Follow-Up

Subject Line: Next Steps: Reducing Human Risk at [Client Name]

Hi [First Name],

Thank you for taking the time to discuss your cybersecurity needs today! As mentioned, we'd love to run a quick Human Risk Report for your team to identify specific vulnerabilities and provide actionable insights on reducing risk.

Let me know a good time next week for us to get started!
Best regards,

[Your Name]

Post-Trial Follow-Up

Subject Line: Results from Your Free Trial with [Your MSP]

Hi [First Name],

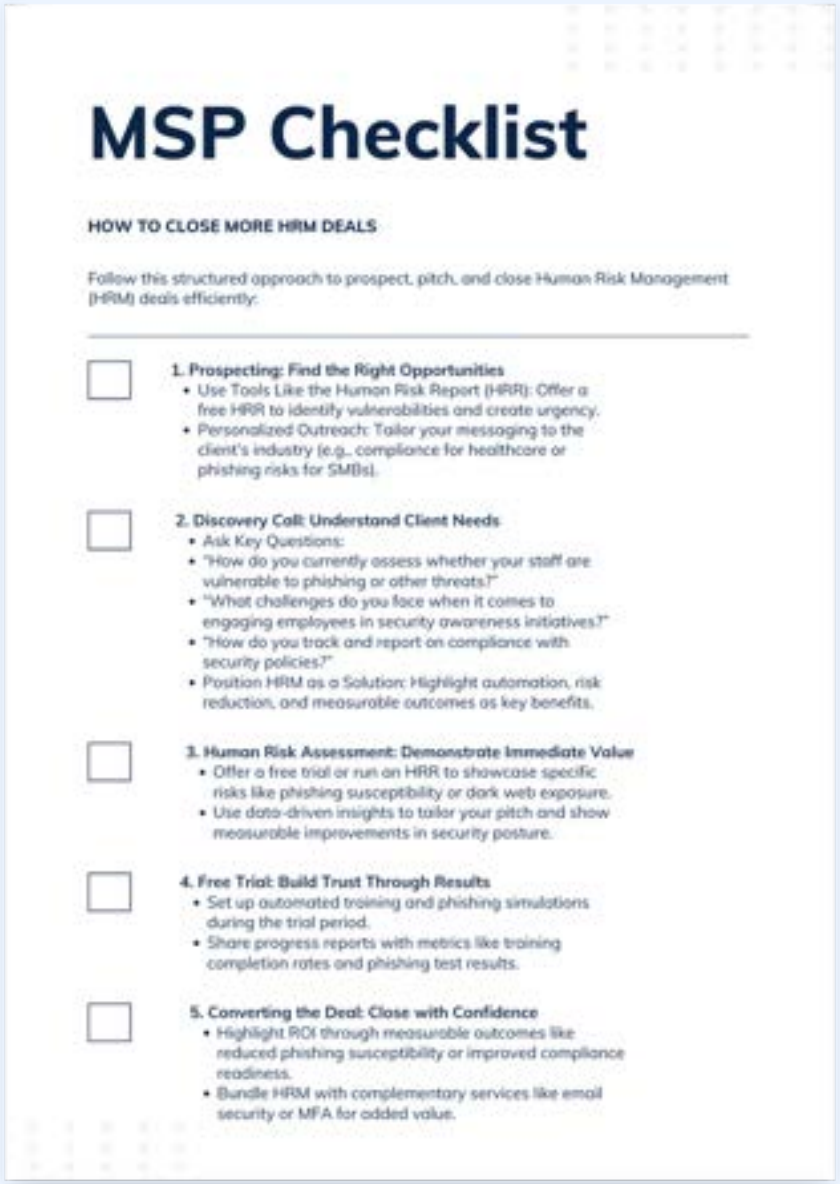
I hope you've had a chance to review the results from your free trial! Here's what we've achieved so far:

- [Metric 1: e.g., % of employees completing training.]
- [Metric 2: e.g., % of phishing simulations successfully identified.]

Based on these results, we'd love to discuss how we can continue reducing human risk across your organization with our full solution.

Let me know when you're available for a quick call!

Best regards, [Your Name]


MSP Checklist

HOW TO CLOSE MORE HRM DEALS

Follow this structured approach to prospect, pitch, and close Human Risk Management (HRM) deals efficiently:

1. Prospecting: Find the Right Opportunities
   - Use Tools Like the Human Risk Report (HRR): Offer a free HRR to identify vulnerabilities and create urgency.
   - Personalized Outreach: Tailor your messaging to the client's industry (e.g., compliance for healthcare or phishing risks for SMBs).
2. Discovery Call: Understand Client Needs
   - Ask Key Questions:
   - "How do you currently assess whether your staff are vulnerable to phishing or other threats?"
   - "What challenges do you face when it comes to engaging employees in security awareness initiatives?"
   - "How do you track and report on compliance with security policies?"
   - Position HRM as a Solution: Highlight automation, risk reduction, and measurable outcomes as key benefits.
3. Human Risk Assessment: Demonstrate Immediate Value
   - Offer a free trial or run an HRR to showcase specific risks like phishing susceptibility or dark web exposure.
   - Use data-driven insights to tailor your pitch and show measurable improvements in security posture.
4. Free Trial: Build Trust Through Results
   - Set up automated training and phishing simulations during the trial period.
   - Share progress reports with metrics like training completion rates and phishing test results.
5. Converting the Deal: Close with Confidence
   - Highlight ROI through measurable outcomes like reduced phishing susceptibility or improved compliance readiness.
   - Bundle HRM with complementary services like email security or MFA for added value.

Download checklist →

Your MSP Sales Success Checklist

To wrap up, here are the three essential principles for selling Human Risk Management successfully as an MSP.

✅ **Speak the Client's Language**

Don't sell "security training"—sell risk reduction and compliance ease.

Example: Instead of "This solution includes phishing training," say, "This solution helps you stop staff from clicking phishing emails in the first place."

✅ **Make It Easy to Buy & Implement**

Position HRM as a fully managed service so clients see it as a hands-off, high-value solution.

Example: "You don't have to do anything manually—our system automatically enrolls, trains, and reports compliance status for you."

✅ **Show Immediate Value**

Use trials and reports to reveal risk exposure instead of just selling training.

Example: "Let's run a quick gap analysis—if you have employees failing phishing tests, we'll fix it before an actual attack happens."

Your 4-Step Action Plan

1. Identify your ideal-fit prospects using the buyer persona guide
2. Run a discovery call to uncover behavior-driven and compliance-based risks
3. Offer a Human Risk Report or trial to deliver immediate, visible value
4. Use the objection-handling framework to close with confidence

You're not selling another tool. You're delivering a smarter, easier way for your clients to reduce human risk and stay secure.

✅ **By following this playbook, you'll:**

- Win more business with strategic positioning
- Boost MRR through HRM-based services
- Retain clients longer with measurable, ongoing value

Explore usecure's solutions

Ready to onboard clients or trial it internally? Request your NFR licence and get started in minutes.

Request a Demo →

Request NFR licence →