

usecure

# The Ultimate MSP Handbook for Selling usecure

Learn how to prospect new clients, sell usecure  
and generate long-term recurring revenue.



# Introduction

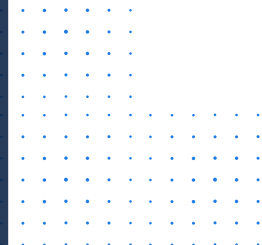
As an MSP, you already know how vital it is for your clients to strengthen their human security posture in order to combat rapidly evolving cyber threats.

But how do you get decision-makers to understand the need to train their users and, more importantly, act now?

In this guide, we'll provide you with tips on how to sell usecure in a way that enhances your service value and drives long-term recurring revenue.

## Contents

- usecure's Differentiators & Benefits
- Common Client Pains VS Gains
- Win New Clients with The Human Risk Report
- Using Tiered Subscriptions - Core VS Advanced
- Bundling usecure with Other Services
- Why Flexible Billing is KEY
- Generating Long-Term Revenue with usecure
- Exploring your Marketing & Sales Resource Hub



# Traditional security awareness is broken. Human Risk Management (HRM) is the fix.

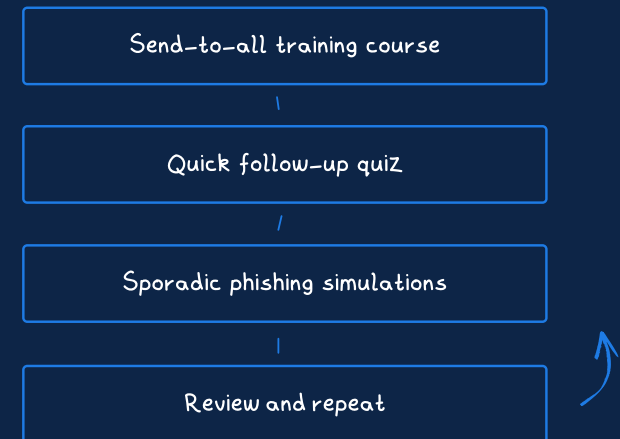
Traditional training is built on the idea that humans are the "weakest link in the cyber security chain". We believe that humans are an organisation's strongest line of defence against evolving cyber threats - you just need the right tools to get them there.

That's why we've built a low-cost, low-admin and fully automated solution that enables businesses to understand and monitor their human risk areas, whilst driving secure human behaviour through user-tailored training, regular phishing simulations and simplified policy management.

## usecure's key differentiators and benefits

- **Admin-lite automation** - Save time and sanity, launch in a flash
  - usecure's automation creates, manages & tracks the training programs for your client
  - No need to spend time on finding relevant courses, chasing staff or sending reports
  - Automate training, phishing, policy approvals, breach monitoring and risk reporting
- **User-tailored training** - Tackle each users' high-risk areas first
  - Every users' training program is tailored to address their unique human risk areas
  - 10-minute Gap Analysis Questionnaire assesses each users' security knowledge
  - Courses are then prioritised for each user depending on where they scored lowest
- **Human risk reporting** - Understand the risks & demonstrate compliance
  - Understand where the human risk areas lie within your business at any one time
  - Track risk over time with individual and company-wide human risk scores
  - Monitor course participation, grades and get weekly summary reports
- **Comprehensive solution** - More than just security awareness training
  - uPolicy keeps staff updated on policies & processes, and tracks signatures
  - Easy external access for auditors makes demonstrating compliance a breeze
  - uBreach detects when user credentials are compromised on the Dark Web

## Traditional security awareness approach



## Automated Human Risk Management (HRM)



### Industry pains

- ✗ Over 90% of data breaches are the result of human error
- ✗ 80% of businesses have experienced an increase in cybercrime
- ✗ Phishing has increased by 667% in 2020
- ✗ Cloud-based attacks are up by 625%
- ✗ Business email compromise fraud is up by 200%

2020 statistics

### How human risk management helps

- ✓ Regular employee training reduces cybersecurity incidents by 70%
- ✓ Even the “least effective” programs have a seven-fold ROI
- ✓ 86% of CISOs listed improving security standards as a top priority
- ✓ 93% of security professionals agree that strong human and machine security protection is the most effective way to prevent disaster

### Common client pains

#### Pains they experience

- ✗ Phishing is more frequent / more difficult for users to spot
- ✗ Poor security behaviour is leaving us at risk of a breach
- ✗ We don't have the budget for a security awareness program
- ✗ Our senior management won't buy into user training
- ✗ Trying to raise security awareness is way too time consuming
- ✗ We need to train staff regularly to satisfy regulatory compliance

#### Gains they want

- ✗ We want to understand our organisation's current human risk
- ✗ We want our staff to understand their security responsibilities
- ✗ We want an efficient way of conducting ongoing user training
- ✗ We want users to proactively report phishing attacks
- ✗ We want to embed a security-minded workplace culture
- ✗ We want to easily demonstrate regulatory compliance

### How usecure helps

#### Pains relieved with usecure

- ✓ Staff are regularly educated and tested on evolving phishing threats
- ✓ Our staff are continuously trained on a range of core infosec topics
- ✓ We've launched low-cost training on a flexible monthly subscription
- ✓ We've generated a free risk report that demonstrates the requirement
- ✓ Our automated training program saves us admin time
- ✓ We satisfy compliance with monthly staff training courses

#### Gains experienced with usecure

- ✓ We can easily monitor our organisation's Human Risk Score
- ✓ Our security awareness training clearly articulates user responsibilities
- ✓ Bite-sized courses are automatically deployed and tracked each month
- ✓ Users know how to spot and report a phishing attack
- ✓ Staff are continuously trained on daily security best practice
- ✓ We track course participation, grades, policy signatures and more

### Many clients already know the risks, so why don't they buy NOW?

Shedding some light on the latest user-related breach statistics and industry fines is helpful for educating prospects and clients, but the truth is, the decision-maker won't really care enough to do anything about it.

That's partly because it's rare for SMB data breaches to make headlines, making it difficult for smaller businesses to relate to these stories and fuelling the misconception that they aren't really a target for cyber criminals.

The most effective way to get decision-makers to act now, is by showing them how at-risk their users already are to common vectors of attack.

### Sell better with the Human Risk Report (HRR)

HRR is the automated sales prospecting tool for MSPs, that calculates the human cyber risk of current and prospective clients in just a few steps, then generates an actionable one-page report that opens a gateway for selling risk management solutions at scale - helping MSPs:

- Generate more leads with a unique service offering
- Initiate better sales conversations with actionable reports
- Demonstrate the urgent need for Human Risk Management
- Win new clients by switching prospects onto a paid account

Launching an HRR is free and is heavily automated, making it quick and easy to start demonstrating human cyber risk with minimal admin training.

[Learn more about The Human Risk Report](#) →

NEW

You can now [add the HRR widget](#) to your website to help you capture more leads and grow your pipeline!

#### How HRR helps MSPs sell better

1 Start generating leads

Access your free marketing pack →

2 Launch your prospect's HRR

Add your prospect in a few clicks →

Domain scan is launched

Dark Web scan is launched

Simulated Phishing Campaign is launched

Human risk is calculated

Human Risk Report is generated →

[View an example report](#) →

3 Convert prospect into a client

Launch free trial / paid account →

## Keeping your tiered subscriptions flexible and simple

We recommend splitting your subscription options into two tiers - Core and Advanced. This should help keep your clients' options flexible, whilst keeping the platform simple to sell.

Both plans require minimal admin time, with automation and readily-made templates pre-loaded into the platform. You can build custom courses, phishing templates and policies in minutes, and then re-use these across multiple clients - helping you grow your margins and value without much additional workload.

Plan	Service		Admin	RRP
<b>Core</b>  <i>Launch an automated program in a flash and start demonstrating value</i>	<b>uLearn</b> Automated user training	<b>uPhish</b> Automated phishing tests	<b>Admin Time = Very Low</b>  Automate everything! Set it and forget it  Launch full program in a flash  Great entry plan for clients who want to test the platform	<b>£2.50</b>  per user/ per month
	<b>uBreach</b> Automated breach scans	<b>Reporting</b> Automated reporting		
<b>Advanced</b>  <i>Enhance value and grow your margins, whilst keeping admin low</i>	<b>uPolicy</b> Policy management		<b>Admin Time = Low</b>  Readily-made phishing and policy templates  Easily build custom courses  Distribute your custom content amongst other clients to save time	<b>£4.00</b>  per user/ per month
	<b>Custom phishing campaigns</b>	<b>Custom user training courses</b>		

✓ Core Plan - is heavily automated, can be launched in a few clicks and takes minimal time to manage - making it a great starter plan to showcase usecure's value.

✓ Advanced Plan - is a great way to offer additional value and increase your margins, with a library of done-for-you templates that keep admin incredibly quick and easy.

### How to bundle usecure with other services

Customers need to know that technical security measures like anti-virus and mail filtering measures aren't a silver bullet for preventing threats like phishing and ransomware.

Ultimately, humans are the first line of defence and they need to be trained to detect threats when technology inevitably fails.

That's why bundling usecure alongside these services will enable your MSP to deliver a fully-rounded security offering that truly enhances the value of your service, whilst better protecting your clients.

- ✔ **Bundle with infrastructure tools** - Package usecure with tools like anti-virus and email filtering.
- ✔ **Sell a 'fully-rounded' security service** - usecure should be embedded as part of a robust security approach that addresses both the technical and human elements of cyber security.
- ✔ **Sell as a full-stack** - Sell usecure as an integrated stack where each element compliments the other.
- ✘ **Avoid itemising** - We don't recommend selling usecure's features individually, as the product stack as a whole provides more security and is easier to sell.



### Why offering your clients flexible monthly billing is key

usecure's flexible monthly billing is designed to have minimal commitments, making it easier for clients to opt in and start experiencing the true value of usecure without worrying about long-term annual subscription costs.

Clients often experience the immediate value by being able to understand their unique human risk areas and knowing exactly how to reduce them. After a few months, usecure is embedded as a standard internal process that is continuously demonstrating impact through ongoing reporting and human risk scoring - which is great for making the platform stick and encouraging long-term use.

#### Why flexible billing is key ↻

- ✔ Simple opt-in - Makes it an easier decision for clients to start testing usecure, without having to commit to long-term cost.
- ✔ Less fear, uncertainty or doubt - Allows clients to test the platform for a few months in order to see the value.
- ✔ Embeds usecure as an internal process - Allows clients to embed staff training into their internal processes during the testing phase, with most clients choosing to continue.
- ✔ Stand out from the competition - A lot of providers only offer annual subscriptions. Making noise about how flexible usecure's subscription plan is a great added benefit and often a key reason that clients choose us.





# 5 golden rules for generating long-term revenue with usecure

---

### 1 Set expectations

Articulate to your clients that the standard of human risk management has changed - Cyber attack techniques are evolving and becoming more prevalent and difficult to spot each year. The requirement for just quick annual security awareness sessions no longer exists. Now, a more robust approach is needed to keep businesses safe, and that involves continual monthly training. Explaining this to your clients will help position usecure as an essential ongoing solution, not a quick fix.

---

### 2 Automate regular training & phishing simulations

**Set AutoEnrol to monthly** - This will ensure that regular courses are deployed and each user's risk level is being continuously reduced through ongoing education.

**Set uPhish to quarterly** - Regular phishing simulations will ensure that employee cyber risk is reducing and that the training is working.

---

### 3 Enhance value

**Integrate uPolicy into their processes** - Automating send-outs and signature approvals when policies are updated or when new staff are hired makes policy management incredibly simple. Once this is embedded into your client's processes, it's unlikely they'll want to return to a more manual approach.

---

### 4 Communicate ongoing threats

**Monitor uBreach to show that the threats are always there** - Monitor uBreach to prove to your clients that, although their human cyber risk is reducing, cyber criminals are always active and trying to find new ways to breach their organisation - and stolen credentials are usually the starting point of attack.

---

### 5 Demonstrate the value

**Use the Risk Score to demonstrate impact** - usecure's reporting is designed to clearly articulate to non-technical decision-makers how human risk is changing. Share regular reports with clients to keep them in the loop on their progress.

## Explore your free Marketing & Sales Resource Hub

We've created a library of whitelabelled resources to help our partners go to market quickly and start selling usecure to existing and potential clients.

Visit your resources below, or go to <https://help.usecure.io/en/>



Technical



Marketing



Sales

### Other useful links:

- [Getting Started with usecure](#) »
- [usecure Knowledge Base](#) »
- [Human Risk Report \(HRR\) Resources](#) »
- [Partner Demo Hub](#) »
- [What's new on the usecure app?](#) »
- [Capture more website leads with the HRR widget](#) »

Links not working? Go to <https://help.usecure.io/en/>