OutThink

Adaptive Security Awareness Training
Autonomous Phishing Simulations
Human Risk Intelligence

CYBERSECURITY HUMAN RISK MANAGEMENT PLATFORM
(SaaS)

EXECUTIVE SUMMARY

Why OutThink?

The world around us is becoming digital, including the way we communicate and protect our information. Today, the vast majority of information security incidents and data breaches are caused by the employees. If you believe in the evolution of information security, it's time to go beyond traditional security awareness and prevent breaches by understanding your people.

Who is OutThink?

OutThink is a London-based company, recognised by Forrester and Gartner for innovation in cybersecurity. OutThink was set up in 2015 by a team of four CISOs – Flavius Plesu., Darren Argyle, Paul Drake and Taewan Park. The research angle is covered by Professor Angela Sasse.

With a perfect 5.0 score, OutThink is the highest rated security awareness solution. The score is based on customer reviews, independently verified by Gartner®. OutThink is also recognised by Forrester® for its innovative capabilities – security culture mapping & human risk quantification.

How OutThink works?

OutThink is a human risk management platform (SaaS) that delivers targeted security awareness training based on employees' needs and level of risk. This is only the first step.

In the process, we get to know the employees - we measure their perceptions, intention to comply, sentiment and psychographic profile. This subjective data comes from employees' interaction with the OutThink learning experiences.

At this point, OutThink is able to identify high risk users, segment the organisation and provide key insights into people's attitudes towards security. This gives the CISO better visibility of human risk across the organisation and answers three fundamental questions:

1. Who are our high-risk groups / employees?
2. Why are these people more likely to cause a security incident / data breach?
3. How can we support them better?

OutThink further integrates with security systems (e.g., SIEM, CASB, EDR, Web Filter, Email DLP) that clients already have in place, to measure security behaviours - objective data.

The OutThink unsupervised machine learning engine analyses subjective data in conjunction with objective data, to anticipate security breaches. We call this predictive human risk modelling, and it is important because it gives security teams the advance warning required to effectively manage the risk of likely security incidents and data breaches.

What OutThink delivers?

OutThink delivers adaptive security awareness training (incl. phishing simulations) to users, giving defenders the overall human risk picture. This provides a solid foundation for risk-based decision making and treatment prioritisation.

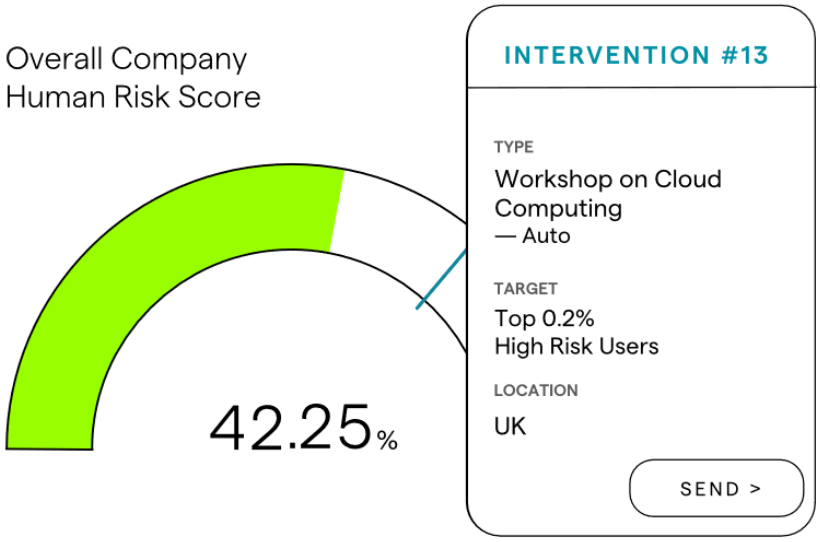
hello@outthink.io
www.outthink.io

OutThink Ltd
+44 (0) 203 4324846

35 New Broad Street
London, EC2M 1NH, UK

1. THE OUTTHINK USP

We address the security challenge from the People perspective by enabling large, complex organisations to prevent data breaches caused by their employees.



Improve Engagement – Give your employees a two-way communication channel, social learning experience to increases engagement.

Measurement – Identify users who are at risk of security incidents. What segments do they fall into and how to engage, how to better support them? With scientific models developed by Dr. Shorful Islam and Professor Angela Sasse; the world's leading voices for human-centred security, it is now possible to demonstrate human risk reduction and programme success.

Manage Human Risk – Understand and manage human risk. OutThink provides both automated (one-click) and manual improvement actions, form historically proven risk treatment methods.

Targeted Interventions – OutThink gives security teams the visibility required to deliver targeted interventions (security awareness training, workshops, reengineer processes, technology, and tools) and manage the risk of data breaches caused by human behaviour more effectively.

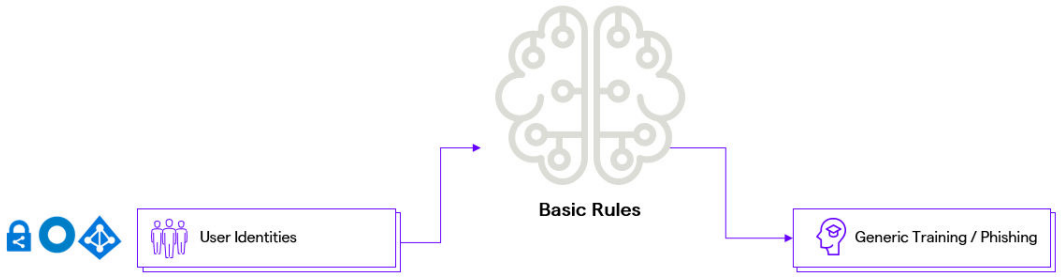
hello@outthink.io
www.outthink.io

OutThink Ltd
+44 (0) 203 4324846

35 New Broad Street
London, EC2M 1NH, UK

2. THE DIFFERENCE

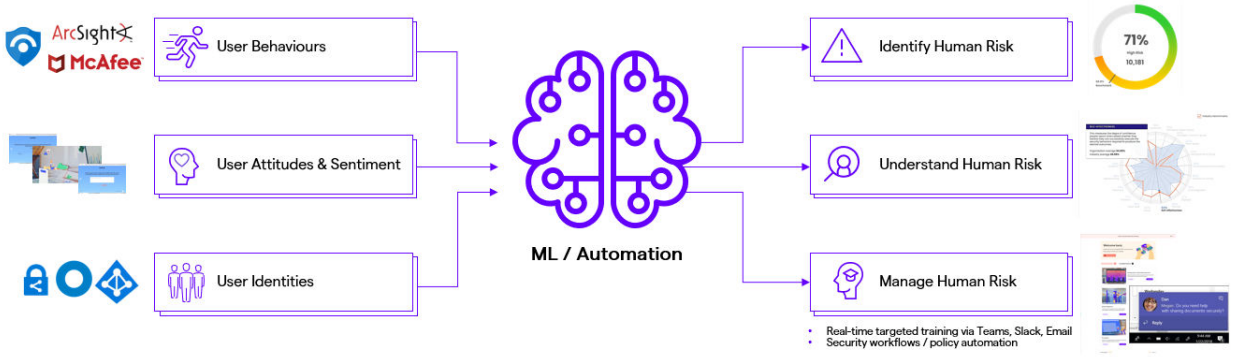
Organisations are looking to reduce the risk of security breaches caused by employees. OutThink can support this by introducing solid measurement and scientific rigour, which will enable better human risk management decisions and drive efficiency.



Traditional SA&T

VS.

Cybersecurity Human Risk Management Platform



FORRESTER®

"The days when SA&T solutions had one purpose, which was to "train" people about security are mercifully disappearing. Clients now buy modern solutions to measure human risk and focus security resources where they are most required."

Forrester Now Tech, Oct 2021

OutThink is committed to helping clients go beyond traditional security awareness training, to achieve long lasting behavioural change. We are very pleased to assist you with maximising the value of your security awareness activities, specifically by:

- Simplifying & automating security awareness
- Delivering phishing simulations with Outlook, O365, G-suite reporting button
- Delivering targeted training, based on employees needs and risk
- Delivering intelligent content directly to the users – via Email or Teams
- Providing unparalleled visibility into the human layer

hello@outthink.io
www.outthink.io

OutThink Ltd
+44 (0) 203 4324846

35 New Broad Street
London, EC2M 1NH, UK

3. WHAT WE BRING

3.1 Adaptive Security Awareness Training

Training that's relevant to your employees, reduces risk and productivity cost.

The eLearning catalogue covers the full spectrum, as certified by the UK GCHQ and NCSC. It comprises of 29 short (5 - 10 min) interactive modules, with 2D animation. The content and user interface is available in 18 languages - Arabic, Czech, Danish, Dutch, English, French, German, Hungarian, Italian, Norwegian, Polish, Portuguese (Brazil / Portugal), Romanian, Slovak, Spanish (Spain / Mexico), Turkish.

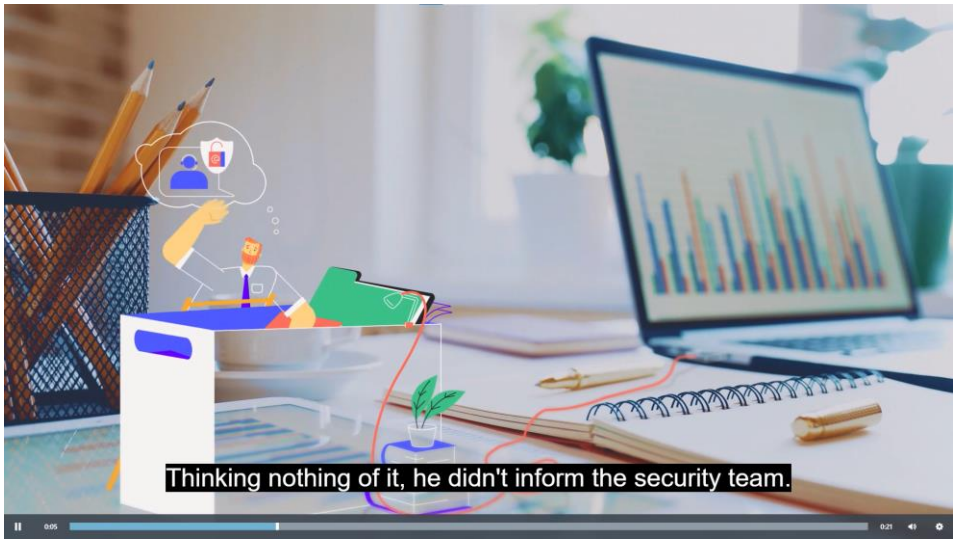
The OutThink dynamic content allocation engine delivers relevant training modules, based on employees' needs and risk. More security, more productivity.

We use storytelling, real life scenarios and characters your employees can identify themselves with. These are accompanied by supporting materials such as short videos, newsletters, screensavers.

OutThink has used an adapted version of Self Determination Theory to gamify the learning experience. High engagement during training, for example submitting a comment, rating a module, completing a module, taking the time to learn (not clicking through) are all rewarded with points. These draw on an individuals' need to demonstrate competence, autonomy, and social relatedness.

Security awareness training topics covered:

- ✓ Introduction to Information Security
- ✓ Email Security & Phishing
- ✓ Web Security
- ✓ Malware Protection
- ✓ Storage Media (portable devices)
- ✓ Cloud Computing
- ✓ Remote Working (public wi-fi use)
- ✓ BYOD & Mobile Device Security
- ✓ Encryption
- ✓ Passwords
- ✓ Social Engineering
- ✓ Social Networking
- ✓ Information Classification
- ✓ GDPR (a suite of 5 modules)
- ✓ Breach Response (incident reporting)
- ✓ Physical Security & Clear Desk



The content can be customised (translations cost), and bespoke modules can be developed (additional cost), if required. New assets are added all the time, to reflect changes in the threat landscape and ensure that your security awareness programme continues to deliver optimal results year after year.
The OutThink security awareness library includes supporting materials such as short videos, posters, screensavers, wallpapers and newsletters.

hello@outthink.io
www.outthink.io

OutThink Ltd
+44 (0) 203 4324846

35 New Broad Street
London, EC2M 1NH, UK

3.2 Phishing Simulations

Phishing is usually the first step in the chain of attack, typically used to drop malware such as ransomware or a key logger. However, even if technical security means exist to prevent phishing, such as email filtering, traffic monitoring and network protection, they cannot be completely effective because phishing involves an unpredictable parameter: human risk.

Most cyber-attacks on organisations start with a phishing email. Initially these emails were easy to recognise, and the security team could easily detect and remove them. Phishing emails have continually improved in design and content and are increasingly more targeted.

In the last few years, we have often seen attractive, legitimate looking emails that used specific information from the organisation or the individual. By clicking on or responding to these emails an employee can potentially give access to confidential information or personal data.

Security departments often cannot detect these phishing emails, but employees can.

With OutThink's phishing simulations, reporting and education you can periodically send phishing emails to employees, monitors and improve their ability to recognise phishing emails over time.

The phishing platform (SaaS) offers the full set of functionalities required to conduct phishing campaigns:

- One-click activation, zero-installation, fully automatic maintenance
- Setup of phishing campaigns
- Creation of phishing email template and landing pages
- Integration and selection of targeted users
- Scheduling of phishing campaigns
- Opt-out process
- Real time monitoring of click rates, time to click, reported etc.
- Evaluation of the basic phishing and ransomware protection controls implemented by the organization
- Final dashboard with consolidated results
- Reporting add-in. The OutThink phishing reporting button seamlessly integrates with your email client. It provides your employees with an easy way to report threats to your security team, from Outlook, O365, G-suite or mobile.

The phishing simulation and associated corporate communications can be optionally complemented by security awareness training focusing on phishing threats. Training can be automatically delivered to repeat clickers.

The email templates encompass approaches commonly used by cyber criminals to best imitate real-world cyber-attacks. The reporting engine generates high-accuracy key metrics which will be provided to senior management.

To safeguard the anonymity of the employees, the click rates are aggregated and reported back to the organisation on a department or country level. In addition, during the test, no sensitive data leaves the organisation's security perimeter.

OutThink understands and removes the legal and execution complexities of a phishing simulation, allowing your organization to focus on its core business in a secure manner.

OutThink proposes a two-pronged methodology which includes both generic and targeted (spear phishing) attacks:

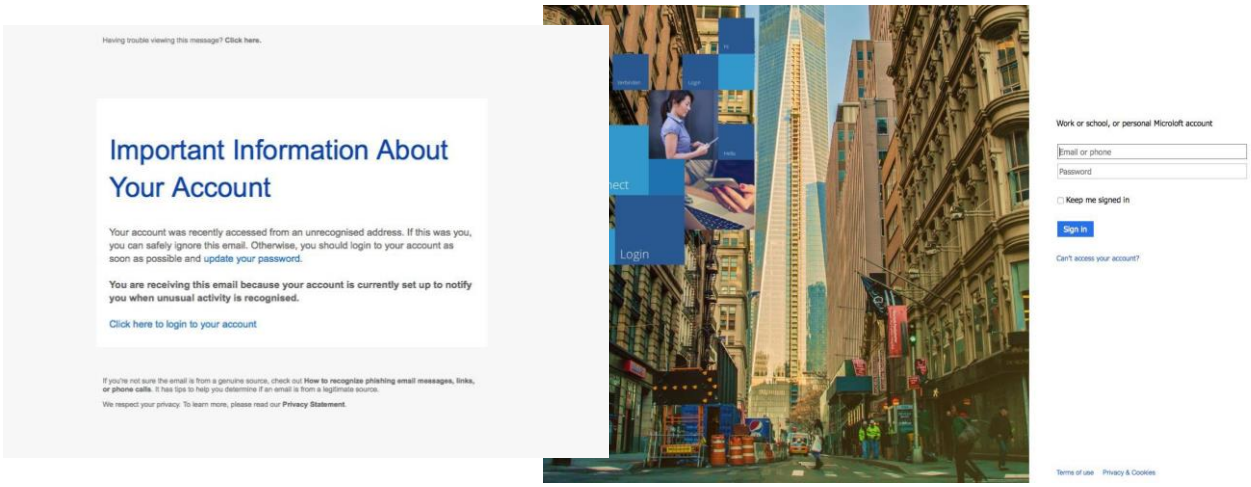
- Generic phishing attacks
- Targeted spear-phishing attacks

hello@outthink.io
www.outthink.io
OutThink Ltd
+44 (0) 203 4324846
35 New Broad Street
London, EC2M 1NH, UK

3.2.1 Generic Phishing

This is the most common form of phishing attack and one that all users of email are likely to be familiar with. Attackers create emails that look like they come from a reputable / trusted sender, for example Amazon, Microsoft, PayPal or internal. There will typically be a call to action but clicking on the link could result in the loss of sensitive information and / or the infection of the user's computer with malicious software.

Targeting all employees with simulated generic phishing attacks will establish a baseline, help understand who needs more support and track long term phishing resilience improvements.



3.2.2 Targeted Spear-Phishing

This attack is more sophisticated and is researched beforehand using social networks and information already in the public domain. Utilising such techniques helps better understand the target and create email templates that will have a higher success rate.

Spear phishing attacks are generally considered a higher risk to the businesses as they are harder for employees to spot if not properly trained. A select number of employees should be targeted with simulated spear phishing attacks, at least quarterly. These simulations should be targeted at high-risk individuals/ departments.

hello@outthink.io
www.outthink.io
OutThink Ltd
+44 (0) 203 4324846
35 New Broad Street
London, EC2M 1NH, UK

3.3 Human Risk Intelligence

Compliance is just the beginning. Go beyond compliance.

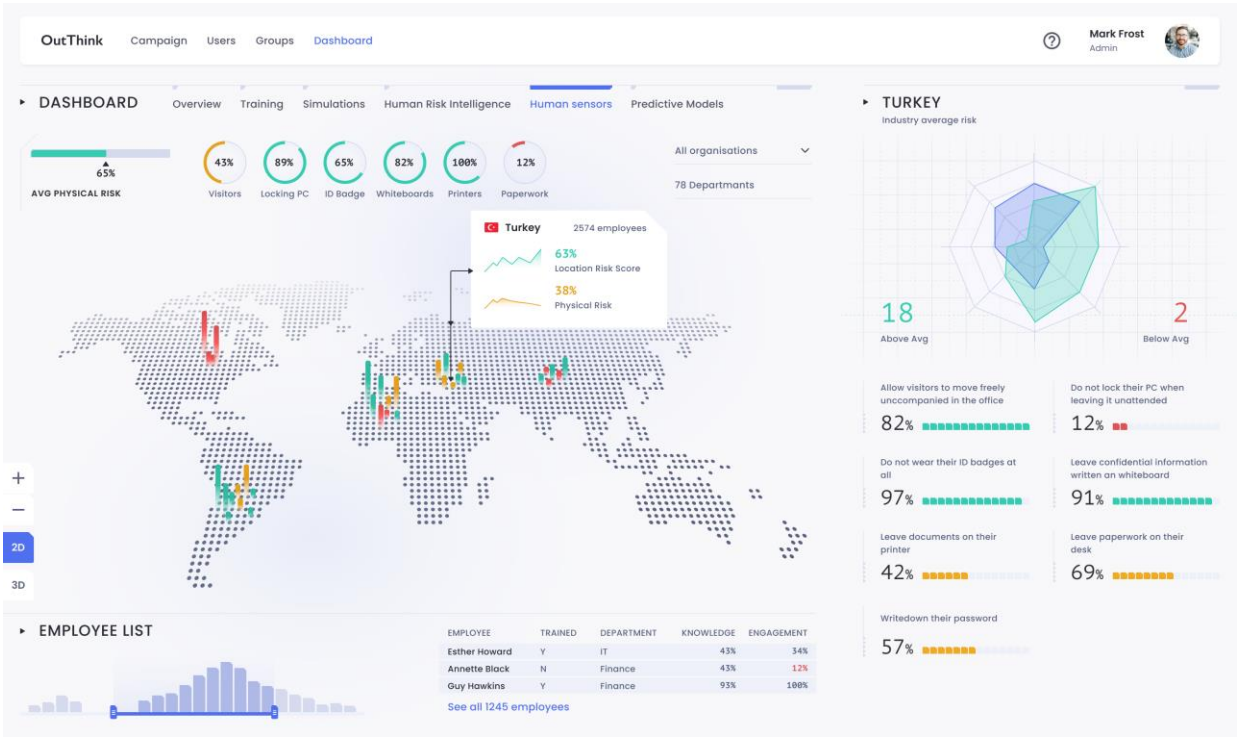
The OutThink algorithms understand individual users, measuring their attitudes (intention, engagement, sentiment, psychographic segment) via telemetry, as they undergo cybersecurity awareness training. OutThink also measures users' security behaviours by integrating with the security systems clients have in place - e.g., EDR, Email DLP, Web Filter, CASB or SIEM.

Using these data sets, the algorithms build an individual's cybersecurity human risk score and, indirectly, the department/division/organisation risk score.

Using OutThink you will be able to identify high risk groups, analyse and understand why are certain people more likely to cause a breach (root cause).

Human Risk Intelligence is critically important because it answers three key questions:

1. Who are our high-risk groups / employees?
2. Why are these people more likely to cause a security breach?
3. How can we support them better?



You can see the change in your human risk exposure in real-time and investigate further if security attitudes / behaviours do not improve.

Visualise human risk, deliver targeted interventions and prevent data breaches like never before. This is the power of human risk intelligence!

hello@outthink.io
www.outthink.io
OutThink Ltd
+44 (0) 203 4324846
35 New Broad Street
London, EC2M 1NH, UK

4. TECHNICAL SET-UP

4.1 Teams Integration

Named administrators are able to create campaigns and are sent campaign alerts, links to organization-wide summary reports via Teams.
We are currently enhancing the Teams App to introduce the ground-breaking concept of delivering real-time interactive modules, nudges, quizzes and surveys directly in Teams. Live learner responses are sent via telemetry to OutThink servers, and supplement the web-based training data, for inclusion in standard reporting and human risk intelligence.

4.2 Azure AD / OKTA Integration

OutThink natively supports the System for Cross-Domain Identity Management (SCIM v2.0). This allows clients to automatically synchronize user populations between compliant identity management solutions (such as Okta, Azure Active Directory or OneLogin) and OutThink.

4.3 EU, UK, US or UAE Hosting, in Azure

The OutThink platform is primarily hosted on the Azure cloud in Europe, with the option of having customer personal data retained within the EU (Netherlands & Republic of Ireland), UK, US or UAE. Global Content Delivery Networks (CDN) and acceleration services ensure a high speed and efficient platform for customers around the world.

4.4 Phishing Reporting Add-In

The OutThink Phishing Reporting Add-In can be centrally deployed to all (or a subset) of your Outlook users via Office Centralised Deployment. The add-in seamlessly integrates with Outlook on the Web (OWA), Outlook Desktop, and Outlook for iOS / Android. OutThink are enhancing the Reporting Add-In functionality to support equivalent functionality within Google Workspace / Gmail.

If a user decides to initiate the reporting action on a particular email, the Add-In will undertake a series of detective actions on the email, and will send relevant telemetry data to the OutThink servers, and/or relay emails to named administrators/SOC team personnel, and quarantine/remove the offending email from the user's inbox. If require OutThink can also integrate with 3rd party phishing reporting button like Cofense, Proofpoint, Knowbe4, Ironscales, etc.

4.5 Integrations with Client Security Systems (Phase 2 – TBC)

OutThink will integrate with security systems clients have in place, to measure user behaviours, by ingesting logs and events on the endpoint, network and cloud.

OutThink analyses this data utilising unsupervised machine learning, based on robust scientific models (behavioural economics & psychology) to predict human risk. The OutThink ML algorithms then recommend improvement actions.

hello@outthink.io
www.outthink.io
OutThink Ltd
+44 (0) 203 4324846
35 New Broad Street
London, EC2M 1NH, UK