Empowering your workforce

5 steps to creating a cybersecurity culture

WAVESTONE

Contents

Handling ever-evolving cybersecurity threats

03

Introducing TAMAM: A Framework For Effective Change

05

Innovative New Approach

12

Handling ever-evolving cybersecurity threats

Picture the scene: Sarah, your busy marketing manager, has just received an email with the subject line, "Urgent: action required re marketing campaign".

It appears to be from your company's CFO, requesting her to click a link and approve a new vendor for an upcoming project. With a looming deadline and an overflowing inbox, Sarah clicks on the link without a second's thought.

Unfortunately, this seemingly harmless action triggers a domino effect. The link leads to a cleverly designed phishing website, which harvests Sarah's login credentials. Hackers then gain access to your company's accounts, steal sensitive data, and launch a serious ransomware attack.

This scenario, though fictional, reflects a troubling trend.

According to the Verizon 2023 Data Breach Investigations Report, **82% of data breaches** involved a human element, with phishing being the most common initial attack vector.

Even with existing awareness training, employees remain susceptible. A recent study by cybersecurity firm Proofpoint found that **one in three employees (33%)*** will click on a phishing email.

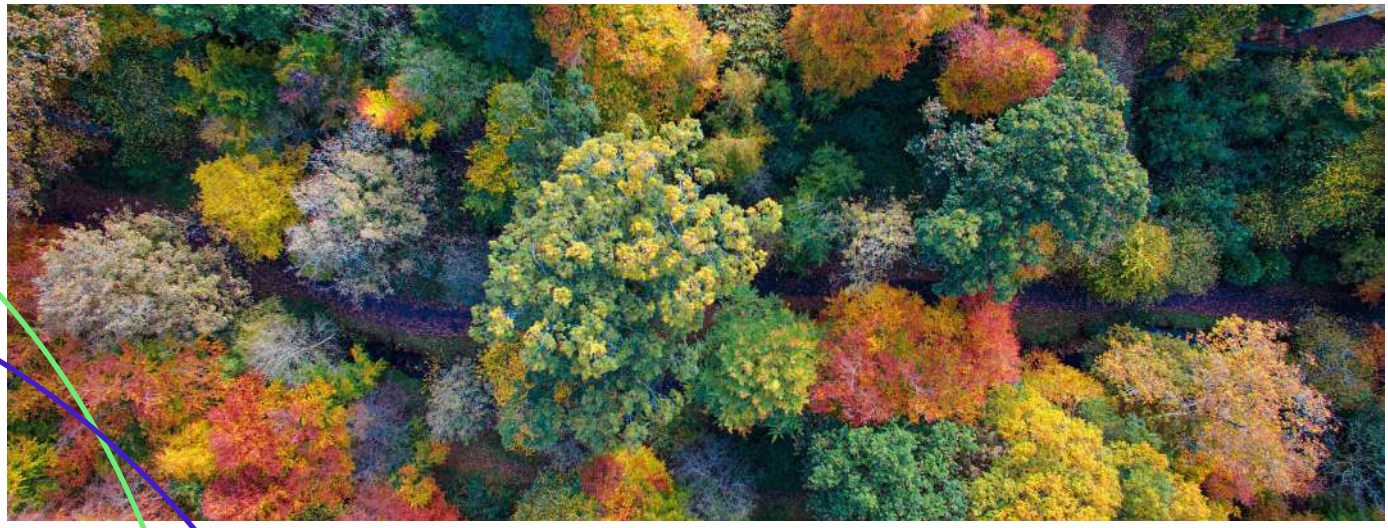
It's hardly surprising. Phishing emails are becoming more and more sophisticated by the day, preying on our time constraints and trust in authority figures.

The cost of these attacks is staggering. Cybersecurity Ventures predicts that global cybercrime costs will reach **$10.5 trillion annually by 2025.** This means businesses of all sizes are at risk, and even a single successful attack can have devastating financial consequences.

So, what can be done?

Traditional cybersecurity awareness training often fails to equip employees with the skills to handle the ever-evolving threats of the digital age. Generic security tips and lectures simply don't resonate with today's workforce.

In this whitepaper, we explore a new approach, and introduce a 5-step framework to help you foster a culture of cybersecurity through a more engaging and impactful awareness programme.



Why traditional methods are failing

Remember the days of mass training sessions and generic "top 10 security tips"? While these methods may have seemed sufficient at first, the rise of sophisticated cyberattacks and the ever-evolving digital landscape have exposed their limitations. Today's employees are bombarded with information, and generic warnings simply aren't enough to change behaviour.

Traditional courses often suffer from:

Lack of engagement

Generic training can be dull and forgettable, failing to capture hearts and minds.

'One size fits all' approach

Not everyone learns the same way. Training courses often fail to cater to different learning styles and employee needs.

A focus on knowledge rather than behaviour

Traditional training tends to focus on theoretical knowledge, which doesn't necessarily translate into real-world application and behavioural change.

Limited measurement

Tracking completion rates doesn't tell the whole story. Traditional methods often lack robust measurement of the actual impact on cybersecurity preparedness.

To address these challenges and ensure your cybersecurity training has maximum impact, a new approach is required. One which empowers your employees to become active participants in safeguarding your business.

Introducing TAMAM: A Framework For Effective Change

Creating a truly effective cybersecurity awareness programme goes beyond one-off training sessions or generic security posters. The challenge lies in fostering lasting behavioural change within your workforce.

Leveraging our extensive experience in cybersecurity programme delivery, our team has developed the innovative TAMAM framework.

Whether you're implementing a company-wide strategy, or require more targeted interventions, this comprehensive, 5-step approach is designed to help you achieve your objectives and cultivate a security-conscious culture.

It can be applied to every organisation, regardless of its size, maturity, budget, or current level of preparedness.

Target:

Clearly define your objectives. What specific behaviours do you want to see from your employees?

Audience:

Segment your workforce based on roles and needs. Tailoring your message ensures it resonates with each group.

Message:

Keep it concise, positive, and action-oriented. Choose a few key messages that address critical risks and desired actions.

Actions:

Go beyond lectures with practical activities and engaging learning experiences.

Measures:

Track progress and measure the impact of your programme on behaviour change.

By following our TAMAM methodology, you can move beyond basic awareness and empower your employees to become active participants in safeguarding your organisation's cybersecurity.

Building a Programme with TAMAM

The following framework is designed to help you develop and implement a programme that drives sustainable behaviour change and strengthens your security defences.

It outlines the 5 key stages of delivering effective cybersecurity awareness and behaviour change.

1. Targets

Simply raising cybersecurity awareness isn't enough. To truly measure the effectiveness of your programme, you need to set clear and actionable targets and communicate them clearly to your audience. Forget generic goals like *"increasing awareness"* - these lack focus and make evaluation difficult. Instead, define specific actions you want your employees to take as a result of the programme.

Here's how to set clear, measurable targets for your cybersecurity awareness programme:

Focus on specific behaviours: Identify the critical security risks your organisation faces and the desired behavioural changes you want to achieve. For example, if phishing attacks are a concern, your target could be: *"Educate employees to report phishing attempts and incidents effectively within 24 hours."* This clearly defines the desired action and sets a timeframe for success.

Quantify wherever possible: Measuring progress against your targets allows you to track progress and assess the programme's effectiveness. or instance, instead of aiming for *"Increased use of phishing awareness training,"* a more measurable target could be *"Reduce the click-through rate on simulated phishing emails by employees from 10% to 3% within 4 months."* This provides a clear baseline (current click-through rate), a desired outcome (reduced susceptibility to phishing attacks), and a timeframe for evaluation.

Align targets with programme objectives: Ensure your targets are directly linked to the overall objectives of your programme. For example, if a programme objective is to strengthen password security, a related target could be *"Increase the percentage of employees using strong passwords (meeting complexity requirements) by 10%."* By aligning targets with objectives, you ensure your programme is working towards achieving its intended outcomes.

Include both leading and lagging indicators: Don't solely rely on lagging indicators, such as the number of reported security incidents (which reflects past behaviour). Look to incorporate leading indicators that assess changes in employee behaviour as a result of the programme. This could include metrics like employee participation in training modules, completion rates for phishing simulations, or the increased use of secure password managers. Analysing both lagging and leading indicators provides a more comprehensive picture of the programme's impact.

Set realistic and achievable targets: While ambitious goals are commendable, avoid setting unrealistic expectations. Consider your budget, resources, and factors such as geographical spread and digital maturity when setting targets.

Communicate targets and objectives transparently: Clearly communicate both the programme's objectives and the associated targets to all stakeholders. This transparency empowers participants to understand the programme's goals, fosters a sense of ownership, and ensures everyone is working towards the same outcomes. By openly sharing the "what" and "why" of the programme, you avoid confusion and create a foundation for success.

2. Audience

One size doesn't fit all when it comes to cybersecurity awareness training. Employees have diverse learning styles, technical skill sets, and varying levels of risk exposure depending on their roles. To maximise programme effectiveness, you should segment your workforce and create targeted content for different groups.

The first step is to gain a clear understanding of your workforce demographics. Analyse roles, technical knowledge baselines, skills gaps, and the specific security risks associated with different departments.

Based on your analysis, segment your workforce into distinct groups with similar risk profiles and learning needs. For example:

New hires: Equip this group with a strong foundation in cybersecurity fundamentals by integrating relevant content into your company's induction process. Focus on basic security principles, company password policies, and acceptable use guidelines. Introduce best practices for identifying phishing attempts and suspicious emails and emphasise the need to report these. You can also cover what not to report – in more mature environments we often see a tendency to over-report non-threatening email such as spam and commercial prospection.

Sales & Marketing teams: These employees are often targeted by social engineering attacks. Develop content that emphasises identifying red flags in social media interactions and recognising phishing attempts disguised as sales leads. Highlight the importance of verifying sender information and exercising caution with unsolicited attachments or links and immediately reporting phishing attempts or click-throughs.

Finance & HR departments: These teams handle sensitive data, making data security paramount. Craft content focusing on data security best practices, encryption protocols, and proper information handling procedures. Train employees on how to identify and report suspicious data breaches or attempts to access confidential information.

Technical teams (IT, Development): This group requires a more in-depth understanding of cybersecurity threats and vulnerabilities. Provide content on advanced security protocols, system hardening techniques, and secure coding practices. Offer training on incident response procedures and best practices for mitigating cyberattacks.

Leadership teams: Leaders hold the key to a strong security culture. Educate them on cyber threats, financial and reputational risks, and the importance of employee engagement. Empower them to not only understand but also embody secure behaviour, acting as role models and cascading key security messages throughout their teams for maximum impact.

Leadership teams: Leaders play a crucial role in fostering a culture of security. Educate them on the importance of cybersecurity, the potential financial and reputational risks of breaches, and the critical need for employee engagement in security initiatives.

3. Messaging

Grabbing and retaining your employees' attention with cybersecurity messaging can be a challenge. With limited time and competing priorities, your messages need to be clear, concise, and impactful.

Here's how to craft meaningful messages that resonate with your employees and encourage positive security behaviours:

Focus on a few key messages: Resist the urge to bombard employees with a laundry list of cybersecurity tips. Instead, identify the **critical risks** your organisation faces and the **desired actions** you want employees to take. Prioritise a handful of key messages that address these specific vulnerabilities.

Positive and action-oriented: Ditch the scare tactics and negativity, instead focusing on the positive impact of good cybersecurity practices. Frame your messages to **empower** employees, highlighting how their actions can protect themselves, their colleagues, and the organisation as a whole. Use action verbs and clear instructions to encourage desired behaviours, e.g. "Always double-check sender addresses before clicking on links", or "Report suspicious emails to the IT security team immediately."

Tailor the message to suit your culture and audience: For a more formal environment, opt for professional and concise language. In a more casual workplace, a friendly and approachable tone might resonate better. Think about how you can repeat your messages in different ways (as different people will respond to different stimuli, which could be practical, visual, spoken, etc.)

Use real-world examples: Employees are more likely to connect with messages that feel relatable. Use real-world examples of cyberattacks and their consequences to illustrate the importance of good security practices. Highlight successful security measures implemented within your organisation to showcase the benefits of vigilance.

Keep it simple: Avoid technical jargon and complex language, and use plain English that everyone can understand. Employees shouldn't need a cybersecurity degree to decipher your messages. Aim for short, impactful messages that can be easily digested and remembered.

Prioritise behaviour change: While accuracy is important, aim for messages that trigger positive security habits, even if they simplify a complex issue. Remember, the goal is action, not an academic debate.

Consistency is key: Don't deliver one-off messages and expect lasting change. Integrate cybersecurity messaging into your regular communication channels. Feature security tips in newsletters, utilise internal social media platforms to share updates, or use digital signage to display short, eye-catching messages.

4. Action

As we've seen, traditional lectures and generic online training often struggle to capture attention and translate into lasting behavioural change. Research suggests that theory alone contributes as little as 10% of overall learning, so prioritise hands-on activities to maximise impact. Here are some engaging approaches to actively involve your employees in the learning process:

Here are some engaging approaches to actively involve your employees in the learning process:

Simulations: Putting knowledge to the test

Move beyond theoretical training by creating realistic phishing simulations that mimic real-world cyberattacks. These simulations can involve emails, phone calls, or even social media messages designed to trick employees into clicking malicious links or revealing sensitive information.

By participating in these simulations, employees can test their awareness and practise their response skills in a controlled environment. Analyse the results to identify areas for improvement and refine your programme accordingly.

Role-playing exercises: Practising real-world scenarios

Learning by doing is a powerful technique. Conduct role-playing exercises that simulate real-world cybersecurity challenges your employees might encounter. For example, role-play scenarios like identifying suspicious emails, reporting a security breach to a manager, or handling a social engineering attempt over the phone.

Through role-playing, employees can develop their critical thinking skills, practise their communication techniques, and build confidence in their ability to handle cyber threats effectively.

Microlearning modules: Bite-sized learning on the go

Today's workforce thrives on short, digestible content. Microlearning modules deliver bite-sized, engaging learning experiences on specific cybersecurity topics. These modules can be accessed easily through eLearning platforms or mobile apps, allowing employees to learn at their own pace and convenience.

Microlearning keeps training sessions focussed and relevant, maximising learning retention without overwhelming employees with lengthy information overload.

Gamification: Turn courses into competitions

Infuse elements of fun and competition into your cybersecurity awareness programme. Gamification involves introducing game-like elements such as points, badges, and leaderboards, transforming learning into an engaging competition. Employees can earn points for completing training modules, participating in simulations, or demonstrating good security practices. Leaderboards can foster healthy competition within teams, further boosting engagement and knowledge retention. Remember, gamification should complement your programme, not replace core training elements.

5. Measures

Simply implementing a cybersecurity awareness programme isn't enough. To truly demonstrate its worth, you need to measure its effectiveness in changing employee behaviour. Management will want to see a return on investment, and the security team will need tangible results.

Moving beyond activity metrics

Many organisations mistakenly focus on activity metrics, such as the number of training sessions delivered, or employees reached. While these figures have their place, they don't tell the whole story. Did the programme actually change how employees behave when faced with cyber threats?

Building a comprehensive evaluation plan

A strong evaluation plan utilises both quantitative and qualitative data.

Here's what you can do:

Quantitative measures: Look beyond training completion rates and focus on metrics that demonstrate a behavioural shift. Track changes in reported phishing attempts, password strength, data breaches, phishing simulation results, and security-related helpdesk tickets. Monitoring these metrics before, during, and after your programme reveals its true impact on employee behaviour.

Qualitative feedback: Conduct surveys and focus groups to gauge employee awareness, confidence in handling cyber threats, and their perception of the programme's effectiveness.

Utilising new data sources

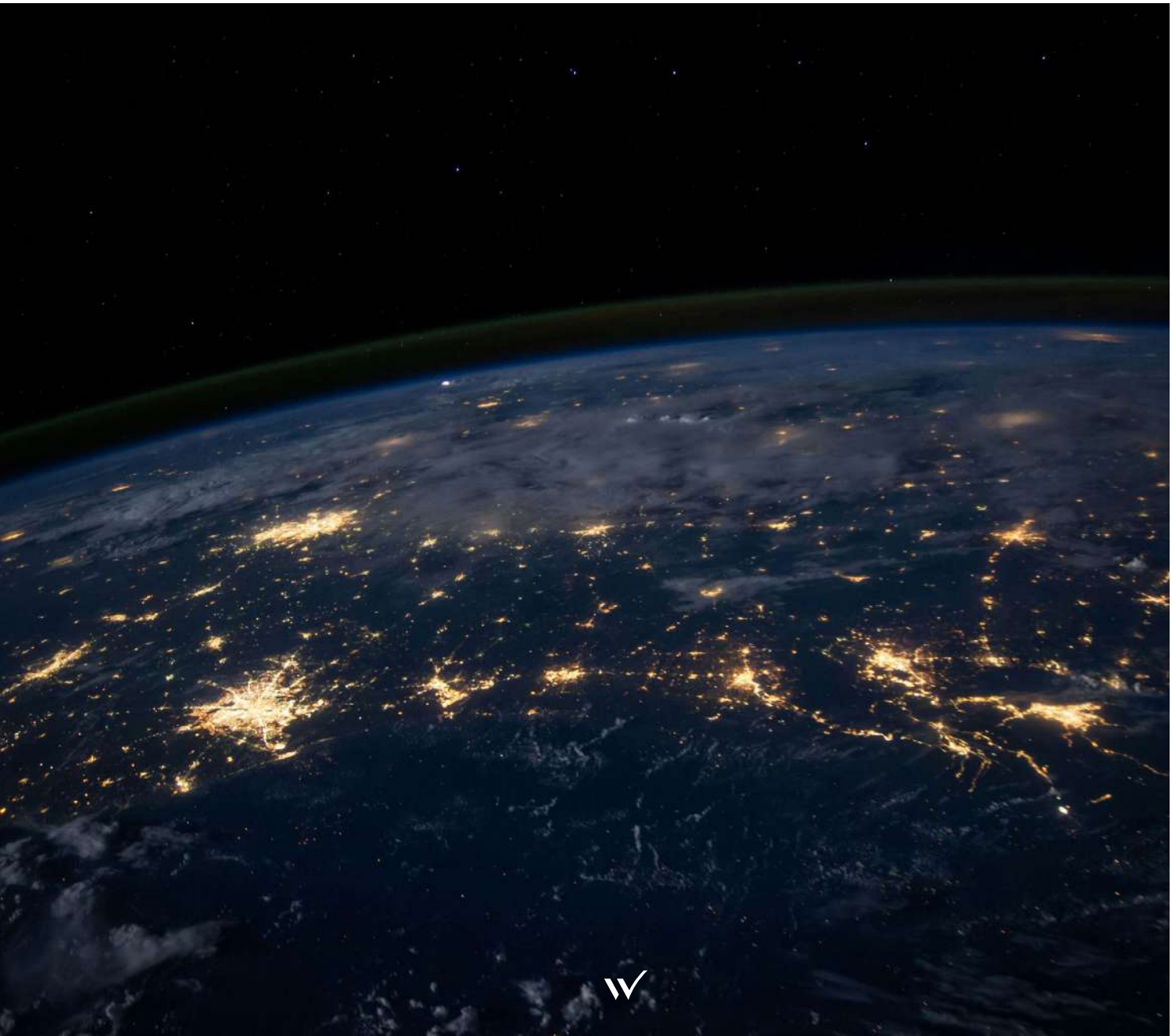
Don't be afraid to explore unconventional data sources. Collaborate with the IT helpdesk to understand the types of cybersecurity issues employees encounter. Consider acquiring fresh data from your Security Operations Centre (SOC) to see if there's a reduction in security incidents.

Continuous improvement through evaluation

The insights from your evaluation are invaluable. They allow you to refine your programme, ensuring it remains aligned with your objectives and adapts to changes within your organisation. Remember, the core goal is to empower employees. Security awareness teams should strive to build confidence and encourage participation, while also establishing clear boundaries about expected behaviours and the limitations of individual actions.

Communicating the positive impact

Once you've collected your data, don't let it gather dust. Clearly communicate the programme's results to stakeholders, highlighting progress made and celebrating wins. This transparency fosters buy-in, motivates employees, and demonstrates the value of the security awareness programme.



Beyond The Programme: Building A Culture Of Security

While a well-designed cybersecurity awareness programme is essential, it's just one piece of the puzzle. Here's how to cultivate a thriving culture of security within your organisation:

Leadership buy-in: Setting the tone from the top

Cybersecurity can't be an afterthought. Secure strong commitment from senior leadership. When leaders visibly champion cybersecurity, it sends a powerful message throughout the organisation. Encourage their participation in videos, webinars, awareness campaigns, internal communications, and even security simulations. This demonstrates the importance of cybersecurity and inspires employees to take ownership of their role in protecting the organisation.

Open communication: Fostering safe spaces for questions and reporting

Employees are often the first line of defence against cyber threats. To empower them, you need to create a culture of open communication. Encourage employees to report suspicious activity or ask questions without fear of reprimand. This can be achieved through anonymous reporting channels, dedicated security awareness email addresses, or open-door policies with the IT security team.

Remember, employees are more likely to report suspicious activity if they feel safe doing so.

Keeping it fresh: Regular communication and engaging content

Cybersecurity messages can become stale quickly. Keep things fresh with regular communication through various channels. Utilise internal newsletters, social media platforms, or even digital signage to deliver bite-sized, engaging content on cybersecurity best practices.

Highlight successful security protocols implemented within your organisation to showcase the benefits of vigilance. Additionally, share real-world examples of cyber threats and data breaches to emphasise the potential consequences of security lapses. This continuous communication keeps cybersecurity top-of-mind and reinforces positive security behaviours.

Recognition and rewards: Celebrating positive security habits

Positive reinforcement goes a long way. Recognise and reward employees who consistently demonstrate good cybersecurity practices. This could include public acknowledgements, awards, or even incentive programmes. Celebrating security champions not only motivates individuals but also inspires others to follow suit.

Communicate your programme's achievements with all employees, highlighting how it's strengthening the organisation's defences. Recognising progress keeps your teams motivated and fosters a positive learning environment.

Beyond training: Ongoing learning and development

Cybersecurity threats are constantly evolving, so your programme should too. Invest in ongoing learning and development opportunities for your employees. Offer access to microlearning modules, online security courses, or lunch-and-learn sessions with security experts. By providing continuous learning opportunities, you empower employees to stay informed and adapt to the ever-changing cybersecurity landscape.

Innovative New Approach

Building a successful cybersecurity awareness programme requires an innovative new approach that is designed with the needs of today's organisations in mind.

The TAMAM framework is a powerful 5-step approach to cultivating a security-conscious culture. By embracing innovation and empowering your workforce, TAMAM transforms your employees into active defenders, significantly bolstering your organisation's cybersecurity preparedness.

To find out how we can help you to design and implement a tailored cybersecurity strategy for your organisation, just get in touch.

*Source: Proofpoint, The Human Factor Report 2023.

WAVESTONE