usecure

Building a Resilient Cybersecurity Culture

How to Build Awareness, Measure Behavior and Reduce Human Risk

www.usecure.io

Table of contents

Executive Summary

> Security awareness remains essential, but completion rates and phishing scores only show part of the human risk picture. Organizations also need to understand how employee behavior connects with credential exposure, identity hygiene, access and the value of the identity being targeted.

The human element was present in 62% of breaches analyzed in Verizon's 2026 DBIR. As attackers expand across email, SMS, voice and AI-assisted social engineering, awareness programs need to evolve from periodic training into continuous, measurable risk reduction.

This white paper explores the impact of security awareness on reducing such risks, offering data-backed strategies to enhance security culture.

Key Findings

- 62% of breaches involved the human element, according to Verizon's 2026 DBIR.
- Simulated voice and text social engineering attacks achieved 40% higher median success rates than email-based simulations.
- Awareness training can improve knowledge and behavior, but Awareness is only one part of human risk.
- Credential exposure, identity hygiene, access and user behavior all contribute to the wider risk picture.
- Human Risk Intelligence connects these signals to show where risk is concentrated and what needs attention first.
- Only 19% of UK businesses conducted staff cyber training or awareness activities, according to the UK Cyber Security Breaches Survey 2025/2026.

Recommendations

- **Build continuous, targeted awareness:** Use assessments and behavioral data to focus learning on the topics and employees that need it most. Keep content relevant as threats change.
- **Make security a shared responsibility:** Leadership should reinforce secure behavior, support participation and make security part of everyday decision-making.
- **Connect awareness with wider risk:** Combine Awareness signals with credential exposure, identity hygiene and access to understand where human risk is concentrated.

Benefits

- **Measurable improvement:** Track how knowledge, phishing behavior and wider human risk change over time.
- **Better prioritization:** Understand which identities and combinations of risk need attention first.
- **Stronger evidence:** Use measurable awareness and risk data to support compliance, reporting and security reviews.

Case Studies

This white paper includes real-world examples of organizations that have successfully integrated security awareness into their operations, illustrating best practices and measurable outcomes, while maintaining compliance with industry regulations.

Security awareness is the foundation, not the finish line

Security awareness gives employees the knowledge and confidence to recognize and respond to threats. A strong security culture makes those behaviors part of everyday work.

But awareness does not exist in isolation. The same behavior can create very different levels of risk depending on the identity involved, their credentials, authentication controls and access.

Why security culture still matters:

- **Safer behavior:** Help employees recognize threats, report suspicious activity and make better security decisions.
- **Compliance support:** Reinforce the awareness and policy requirements built into many security frameworks.
- **Business resilience:** Reduce avoidable exposure and build confidence with customers and stakeholders.

Necessary Components in Building a Good Security Culture:

- **Leadership Commitment:** Executives must lead by example, demonstrating the importance of security through their actions and communications.
- **Continuous Education:** Regular training sessions and updates on emerging threats ensure that employees remain informed and vigilant.
- **Open Communication:** Encouraging feedback and dialogue about security practices fosters a sense of ownership and responsibility among employees.
- **Policy Reinforcement:** Integrating security into company values and policies helps embed it into the organizational DNA.
- **Recognition and Incentives:** Rewarding employees for proactive security behaviors can enhance engagement and participation in security initiatives.

What Does Security Awareness Training Cover?
Security awareness training equips employees with the essential knowledge and skills to protect themselves and their organizations from cyber threats. This training is crucial for reducing security breaches caused by human error and fostering a culture of vigilance.

Effectiveness of Security Awareness Training

Security awareness training is a crucial component in reducing vulnerabilities within organizations. Effective security awareness can improve knowledge, phishing resilience and reporting behavior over time. The strongest programs combine regular training with realistic testing and continuous measurement.

What effective security awareness should cover

Cybersecurity basics

- **Foundational Knowledge:** Employees gain a basic understanding of cybersecurity concepts, including threats like phishing, malware, ransomware, and social engineering.
- **Physical Security and Data Breaches:** Training covers safeguarding physical assets and understanding data breach implications.
- **Public Wi-Fi Safety and Remote Work Guidance: Safer everyday behavior** for safely using public Wi-Fi and securing remote work environments are emphasized.

Threat recognition

- **Identifying Suspicious Activities:** Employees learn to recognize security threats such as phishing emails, fake websites, or unusual system behavior.
- **Phishing Awareness:** Given its prevalence, special focus is placed on recognizing and responding to phishing attempts.

Safer everyday behavior

- **Password Security:** Training emphasizes creating strong passwords and using multi-factor authentication.
- **Data Handling:** Secure handling of sensitive data and keeping systems updated are key components.

Policies and responsibilities

- Employees are familiarized with organizational security policies, procedures, compliance requirements, and their roles in maintaining security measures.

Understanding human risk

- Training helps employees understand the impact of their actions on organizational security posture and encourages proactive risk minimization.

Reporting and response

- Guidance on responding to security incidents, including reporting procedures and mitigation steps.

Continuous learning

- Continuous learning through regular updates on emerging threats ensures employees remain vigilant against evolving risks

Security awareness training can yield a

37-fold ROI

with even the least effective programs offering a 7-fold ROI[4].

Awareness is one signal

Training can show what employees know and where knowledge gaps exist. Phishing simulations can show how they behave.

But neither tells you the complete risk around an identity.

Human Risk Intelligence adds context such as credential exposure, identity hygiene and access, helping teams understand where Awareness weaknesses matter most.

Current human risk landscape

Human risk is becoming more connected. Attackers increasingly combine social engineering, credential abuse, identity compromise and multiple communication channels to reach their targets.

The human element remains significant

Human error continues to be a major factor in cybersecurity incidents. The human element was present in 62% of breaches analyzed in Verizon's 2026 DBIR, while social engineering represented 16% of breaches. This reinforces the importance of helping employees recognize and respond to evolving threats.

Social engineering is moving beyond email

Voice and text phishing simulations recorded 40% higher median success rates than email-based simulations, while smishing increased 40% between Q1 and Q2 2026.

Attackers increasingly combine email, SMS, voice and impersonation techniques. Training should reflect the range of social engineering channels employees now encounter.

- **Business Email Compromise (BEC):** A sophisticated scam targeting businesses working with foreign suppliers or regularly performing wire transfer payments. Attackers compromise or spoof business email accounts to conduct unauthorized fund transfers.
- **CEO Fraud:** A specific type of BEC where cybercriminals impersonate company executives to deceive employees, vendors, or customers into transferring funds or sensitive information.

Impact of Security Awareness Training

In the UK, only 19% of businesses conducted staff cyber training or awareness activities in the previous 12 months, rising to 54% of medium businesses and 84% of large businesses.

62% of breaches involved the human element

Identity makes the difference

A social engineering failure becomes more significant when it overlaps with exposed credentials, weak authentication or elevated access. Understanding the person and identity behind the behavior is critical to understanding the potential impact.

Understanding the importance of a robust security culture naturally leads us to explore how organizations can support this culture through effective training programs. By equipping employees with essential skills and knowledge, training serves as a cornerstone in building a resilient cybersecurity posture.

Why awareness programs can still leave gaps

Despite its importance, effective security awareness training can be difficult to deliver. Just 19% of UK businesses provided staff cyber training or awareness activities in the past 12 months.[5]

The challenge is not only getting employees trained, but understanding whether that activity is reducing risk

While security awareness training is essential, implementing these programs is not without its obstacles. Understanding these challenges is key to developing effective strategies that ensure successful adoption and engagement.

Common Obstacles Faced by Businesses

Organizations often encounter the following hurdles when implementing security awareness programs:

- **Disconnected signals:** Training, phishing, credential exposure and identity data are often viewed separately.
- **Completion is not behavior:** Finishing a course does not necessarily show how someone will respond to a real threat.
- **Threats keep changing:** Social engineering now spans email, SMS, voice and AI-assisted impersonation.
- **Engagement varies:** Generic or repetitive training can struggle to stay relevant.
- **Risk differs by identity:** The same behavior can represent very different risk depending on access, hygiene and exposure.
- **Prioritization is difficult:** Without connected context, teams can struggle to know which users and weaknesses need attention first.

Advanced Phishing Techniques

As cybercriminals become more sophisticated, phishing attacks have evolved beyond simple email scams. Understanding these advanced techniques is crucial for effective security awareness training:

- **Spear Phishing:** Highly targeted attacks using personal information to appear more credible. For example, an attacker might impersonate a colleague or vendor, using details gleaned from social media or company websites.
- **Whaling:** A form of spear phishing targeting high-level executives. These attacks often involve extensive research to craft convincing messages that appear to come from trusted sources.
- **Clone Phishing:** Attackers create nearly identical copies of legitimate emails, replacing original links or attachments with malicious ones. This technique exploits familiarity and trust in known senders.
- **Voice Phishing (Vishing):** Phone-based attacks where criminals pose as legitimate entities to extract sensitive information. These attacks often combine with email phishing for increased credibility.
- **SMS Phishing (Smishing):** Similar to email phishing but conducted via text messages. These attacks often exploit the perceived trustworthiness and immediacy of SMS communications.

Small Business Security Awareness Challenges

- **Limited Resources:** Smaller budgets and fewer dedicated IT staff make it challenging to develop and maintain comprehensive training programs.
- **Lack of Expertise:** Without in-house cybersecurity experts, small businesses may struggle to create relevant, up-to-date training content.
- **Perceived Invulnerability:** Many small business owners believe they're not targets for cyberattacks, leading to a lack of prioritization for security awareness.
- **Supply Chain Vulnerabilities:** Small businesses are often part of larger supply chains, making them attractive targets for attackers seeking to breach larger organizations.

Addressing these challenges requires tailored approaches, such as leveraging cloud-based training solutions, partnering with managed security service providers, and fostering a culture where every employee understands their role in cybersecurity.

Overcoming employee resistance

19% 19% of UK businesses conducted staff cyber training or awareness activities in the previous 12 months. Even where training exists, organizations can still struggle to connect awareness activity with wider human risk.

While the benefits of security awareness training are clear, organizations may face resistance from employees. To address this challenge effectively, consider implementing the following strategies:

Management Support:

- Ensure visible endorsement from top leadership to emphasize the importance of security awareness.
- Have executives participate in training sessions alongside employees to lead by example.

Employee Involvement:

- Form a "Security Ambassador" program, allowing interested employees to take a more active role in promoting security awareness.
- Conduct surveys or focus groups to gather employee feedback on training content and delivery methods, incorporating their suggestions to improve engagement.

Contextual Learning:

- Tailor training content to specific job roles, demonstrating how security practices relate directly to employees' daily tasks.
- Use real-world examples and case studies relevant to your industry to illustrate the impact of security breaches.

Continuous Communication:

- Implement a regular security newsletter or intranet section to keep cybersecurity top-of-mind.
- Use multiple channels (email, posters, screensavers) to reinforce key security messages throughout the workplace.

By addressing resistance proactively and making security awareness relevant and engaging, organizations can foster a culture where cybersecurity becomes an integral part of every employee's mindset and daily routine.

38% of UK businesses experienced phishing attacks in the previous 12 months

Case Study – Mentor Group's Success with usecure

At a Glance

- ISO Audit Success: The Mentor Group's training strategy earned high praise during the ISO/IEC 27001 audit.
- User Score Improvement: 34% increase in user scores after implementation.
- Phishing Detection Enhancement: Average phishing compromise rate decreased by 29% in the first year.
- Training Engagement: 94% course completion rate among employees.

About Mentor Group

Mentor Group, a business consulting firm specializing in sales enablement, sought ISO/IEC 27001 accreditation to maintain client trust and demonstrate robust information security practices. This required comprehensive security awareness training tailored to employee roles and data access levels.

The Challenge

- Achieving ISO/IEC 27001 accreditation.
- Ensuring all staff received relevant information security training.
- Demonstrating compliance and improving security behavior through insightful reporting.

The Solution

Mentor Group implemented usecure's comprehensive human risk management solution, which included:

- Automated Training (Auto Enrol): Regular, bite-sized video courses on core information security topics delivered directly to employees' inboxes.
- Phishing Simulations (uPhish): Automated phishing tests using realistic templates to enhance employees' ability to identify phishing threats.

Read full case study here

Results

Mentor Group's use of usecure significantly enhanced their security awareness culture:

- **User Score Improvement:** Average scores increased by 34% after training.
- **Decreased Phishing Compromise Rate:** Dropped by 29% in the first year.
- **High Training Engagement:** Achieved a 94% course completion rate.

Regular, bite-sized training courses not only improved employee knowledge but also fostered a culture of vigilance regarding cybersecurity.

Key Takeaways

- Regular, tailored training is essential for compliance with standards like ISO/IEC 27001.
- Comprehensive reporting and user engagement are critical for demonstrating effective training programs.
- Investing in a holistic human risk management solution can significantly improve security awareness and reduce phishing risks.

Get Started with usecure

Empower your organization like Mentor Group did. Explore how usecure's award-winning Human Risk Management solution can enhance your cybersecurity strategy.

Want to see our Human Risk Intelligence platform in action? **Book a demo today.**

This case study demonstrates how strategic implementation of usecure's solutions can lead to significant improvements in cybersecurity awareness and compliance.

1.Company Culture

Creating a security-aware culture involves integrating security awareness into an organization's fabric. This process ensures that security becomes part of daily operations and decision-making.

2. Leadership

Successful integration starts with leadership. Executives must prioritize security through actions and communications. This top-down approach helps cultivate a culture where security is valued at all levels.

3. Education

Regular training sessions and open communication channels are vital. Employees should be kept informed about threats, as companies such as Google have done through ongoing programs adapting to emerging risks.

4. Reinforcement

Reinforcing security through company values is crucial. Organizations like Microsoft have embedded it into core values as part of their corporate identity.

5. Initiatives

Engaging employees transforms them from passive recipients into proactive stakeholders in cybersecurity efforts.

10 Strategies to Build a Security Awareness Culture

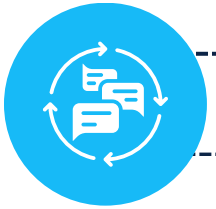
6. Gamification

Introducing gamification elements like leaderboards or rewards boosts engagement. Gamification strategies include:

- **Security Quests:** Create a series of cybersecurity challenges that employees can complete, earning points or badges for each successful task.
- **Leaderboards:** Implement department or company-wide leaderboards to foster friendly competition in security knowledge and practices.
- **Simulation Exercises:** Conduct regular phishing simulations, rewarding employees who successfully identify and report suspicious emails.

Incentive Programs:

- **Recognition Awards:** Establish a "Security Champion of the Month" program to recognize employees who consistently demonstrate excellent security practices.
- **Tangible Rewards:** Offer small prizes or gift cards for employees who achieve perfect scores on security assessments or contribute to improving security processes.
- **Career Advancement:** Consider security awareness achievements in performance reviews and promotion decisions.



7. Regular Feedback

Regular Feedback and Involvement:

Encouraging regular feedback and active involvement from employees is essential for fostering a robust security culture. By creating an environment where employees feel empowered to share their insights and experiences, organizations can enhance their security posture and drive continuous improvement.

Encouraging Feedback includes:

- **Open Communication Channels:** Establish clear and accessible channels for employees to provide feedback on security practices and training programs. This can include suggestion boxes, regular surveys, or dedicated meetings.
- **Feedback Integration:** Actively incorporate employee suggestions into security policies and training content. Demonstrating that feedback leads to tangible changes can increase employee engagement and buy-in.

10 Strategies to Build a Security Awareness Culture

8. Fostering Ownership

- **Empowerment Through Participation: I**nvolve employees in the development and refinement of security initiatives. This can be achieved by forming cross-departmental security committees or task forces that include representatives from various roles.
- **Recognition Programs: A**cknowledge and reward employees who actively contribute to enhancing security measures. Recognition can be in the form of awards, public acknowledgment, or incentives.

9. Education

- **Iterative Training Updates:** Use employee feedback to regularly update and improve training materials, ensuring they remain relevant and effective.
- **Collaborative Problem Solving:** Encourage teams to work together to identify potential security vulnerabilities and develop solutions. This collaborative approach fosters a sense of shared responsibility for organizational security.

10. Involvement

By prioritizing regular feedback and involvement, organizations can cultivate a proactive security culture where employees are not only aware of threats but also actively engaged in mitigating them.

Training Frequency and Engagement

The frequency and engagement level of training sessions are critical to their success. Security awareness works best as a continuous program rather than a one-time exercise. Regular learning, testing and reinforcement help organizations identify persistent gaps and track improvement over time.

With these strategies in place, organizations must also focus on monitoring and measuring the success of their initiatives to ensure continuous improvement and adaptation to new challenges.

Monitoring and Measuring Success

To effectively measure the success of security awareness programs, organizations should track specific key performance indicators (KPIs). These metrics provide valuable insights into the program's impact and highlight areas for improvement:

1. **Phishing Simulation Results:** Monitor the number of employees who fall for simulated phishing attacks over time. A decreasing trend indicates improved awareness and response skills.
2. **Reduction in Security Incidents:** Track the frequency and severity of security incidents before and after implementing the training program. A reduction signifies enhanced employee vigilance and the effectiveness of the training.
3. **Employee Risk Scores:** Use risk scoring to assess individual or departmental vulnerability levels. Improvements in these scores reflect increased awareness and adherence to security protocols.
4. **Training Completion Rates:** Measure the percentage of employees completing training modules on time. High completion rates suggest effective engagement strategies.
5. **Incident Response Times:** Evaluate how quickly employees report or respond to potential threats. Faster response times indicate better preparedness and understanding of security protocols.

These KPIs help organizations assess the effectiveness of their security awareness programs and identify areas needing additional focus.

Measuring Success (KPIs)

Monitoring and Measuring Success

To effectively measure the success of security awareness programs, organizations should track specific key performance indicators (KPIs). These metrics provide valuable insights into the program's impact and highlight areas for improvement:

1. **Phishing Simulation Results:** Monitor the number of employees who fall for simulated phishing attacks over time. A decreasing trend indicates improved awareness and response skills.
2. **Reduction in Security Incidents:** Track the frequency and severity of security incidents before and after implementing the training program. A reduction signifies enhanced employee vigilance and the effectiveness of the training.
3. **Employee Risk Scores:** Use risk scoring to assess individual or departmental vulnerability levels. Improvements in these scores reflect increased awareness and adherence to security protocols.
4. **Training Completion Rates:** Measure the percentage of employees completing training modules on time. High completion rates suggest effective engagement strategies.
5. **Incident Response Times:** Evaluate how quickly employees report or respond to potential threats. Faster response times indicate better preparedness and understanding of security protocols.

These KPIs help organizations assess the effectiveness of their security awareness programs and identify areas needing additional focus.

Continuous Improvement Strategies

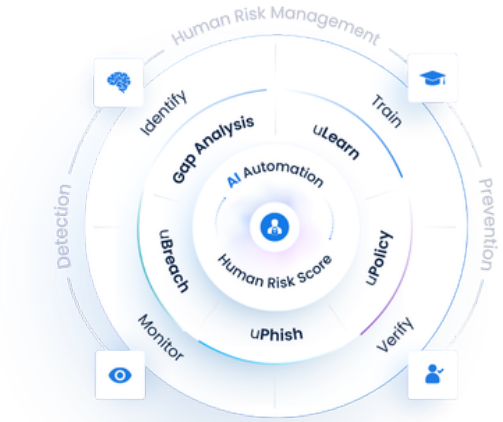
Ensuring continuous improvement in security awareness programs is essential for maintaining their effectiveness over time.

Here are strategies businesses can adopt:

1. **Regularly Update Training Materials:** Keep training content current by incorporating the latest cybersecurity trends and threat intelligence.
2. **Solicit Employee Feedback:** Encourage employees to provide feedback on training effectiveness and areas for enhancement.
3. **Incorporate Behavioral Analytics:** Use analytics to understand employee behavior patterns related to security practices.
4. **Benchmark Against Industry Standards:** Regularly compare your program's performance against industry benchmarks.
5. **Foster a Culture of Continuous Learning:** Encourage a mindset of ongoing learning by offering advanced training opportunities for employees who demonstrate high engagement or interest in cybersecurity topics.

Importance of Continuous Improvement

Continuous improvement is vital for maintaining the effectiveness of security awareness programs. Continuous improvement depends on regularly reviewing training performance, phishing behavior and other risk signals, then adapting the program as threats and employee needs change.



Furthermore, the adaptability of usecure's tools ensures that organizations of all sizes and across various industries can tailor the implementation to their specific needs and risk profiles. Security awareness training management is an ongoing cycle that requires continuous attention and adaptation. By leveraging usecure's comprehensive platform, organizations can effectively manage each stage of this cycle.

Conclusion

Security awareness remains foundational to reducing human risk. Regular, relevant training helps employees recognize threats, make safer decisions and build stronger security habits.

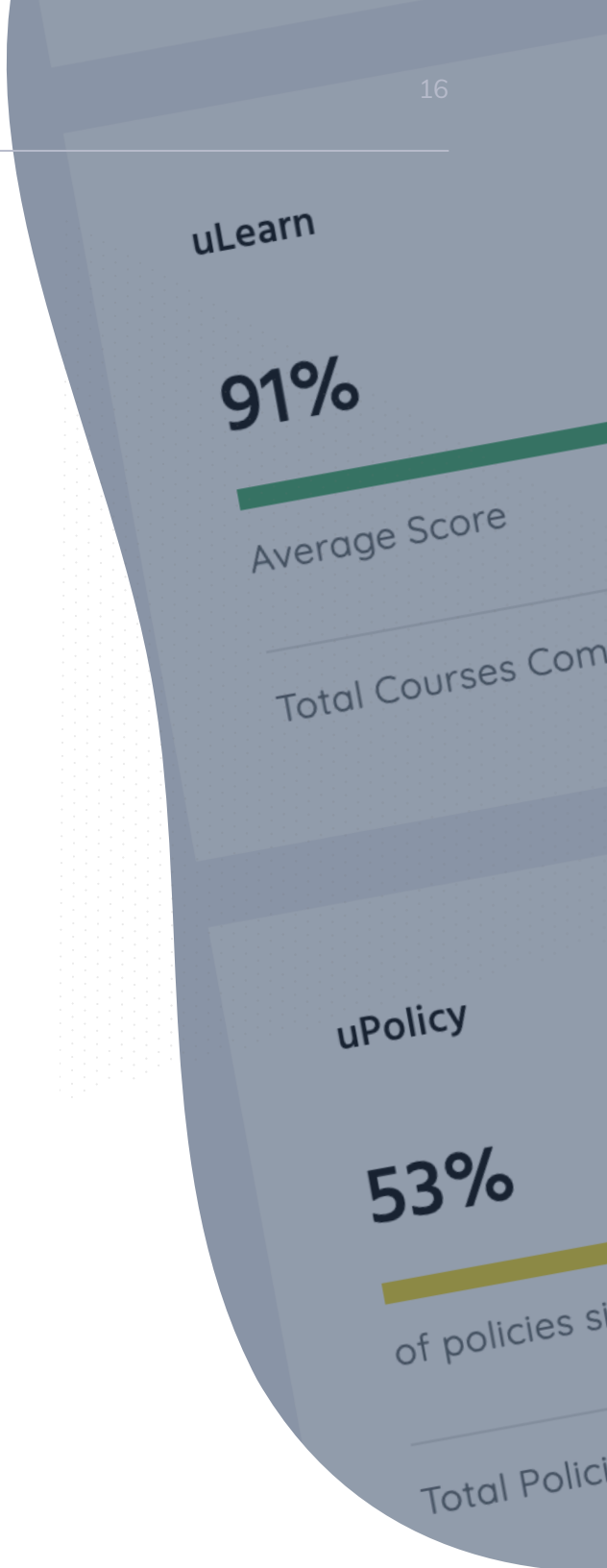
But awareness alone does not show where risk is concentrated. Connecting Awareness with credential exposure, identity hygiene and access provides the wider context needed to understand which identities need attention first.

By combining continuous awareness with Human Risk Intelligence, organizations can move beyond completion rates and isolated scores toward measurable, ongoing improvement.

Key takeaways:

- **Security awareness remains essential:** Regular training helps employees recognize and respond to evolving threats.
- **Behavior matters more than completion:** Assessments, simulations and reporting provide stronger evidence than course completion alone.
- **Human risk extends beyond Awareness:** Credential exposure, identity hygiene and access add important context.
- **Threats continue to evolve:** Social engineering now spans email, SMS, voice and AI-assisted impersonation.
- **Continuous improvement matters:** Training and testing should adapt as threats and employee needs change.
- **HRI connects the signals:** Human Risk Intelligence helps teams understand where risk is concentrated and what needs attention first.

> By implementing these strategies, organizations can cultivate a proactive security culture where employees are not only aware of threats but also actively engaged in mitigating them. This approach not only protects organizational assets but also positions businesses for sustained success in an increasingly interconnected world.



Appendix

1. Verizon 2026 Data Breach Investigations Report
2. UK Cyber Security Breaches Survey 2025/2026
3. APWG Phishing Activity Trends Reports
4. Microsoft Digital Defense Report 2025
5. Human Risk Intelligence
6. Toxic Combinations in Human Risk Intelligence
7. Mentor Group case study

usecure