usecure

Building a Resilient Cybersecurity Culture

How to Drive Security Awareness in Your Business

Table of contents

Executive Summary

> “Security awareness is a critical component of modern business operations, with human error continuing to account for a significant portion of data breaches.”

In 2023, 68% of breaches involved non-malicious human actions (Verizon 2024 Data Breach Investigations Report)[1].

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

Key Findings

- Human error is the main cause o**f 95%** of cybersecurity breaches[2], with **68%** of all breaches in 2023 involving non-malicious human actions[1].
- Over **40%** of successful social engineering attacks were Business Email Compromise (BEC) or CEO Fraud[1].
- 80% of organizations reported a reduction in phishing susceptibility following security awareness training[3].
- Regular training can reduce risk from **60% to 10%** within the first **12 months[4].**
- Companies consistently engaging in security awareness training have seen a **70% reduction in security incidents[5].**
- Security awareness training can yield a **37-fold ROI,** with even the least effective programs offering a 7-fold ROI[4].
- Despite the benefits, 45% of employees report receiving no security training from their employers[1].

Recommendations

- **Implement Comprehensive Training Programs:** Develop adaptive and continuous training programs tailored to the specific risks faced by different departments and aligned with regulatory frameworks such as GDPR, ISO 27001, and the NIST Cybersecurity Framework.
- **Engage Leadership and Employees:** Foster a top-down approach where leadership actively promotes security awareness, embedding it into company culture while ensuring compliance with cybersecurity regulations.
- **Utilize Technology Solutions:** Leverage platforms like ours to deliver customized, effective training that meets the diverse needs of businesses across industries and helps organizations stay compliant with industry standards.

Benefits

- **Risk Reduction:** By prioritizing security awareness, businesses can significantly reduce the risk of data breaches and remain compliant with regulatory requirements.
- **Enhanced Cybersecurity Posture:** Strengthening cybersecurity measures fosters a culture of vigilance and responsibility among employees, while adhering to critical industry regulations.
- **Trust Building:** A proactive approach to both security and compliance safeguards sensitive information and strengthens trust with clients and stakeholders.

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.

Understanding security awareness and culture

In the modern digital era, security awareness is a critical pillar for safeguarding business operations. It encompasses the knowledge and practices that individuals within an organization adopt to protect sensitive data and systems from cyber threats. As cyber threats continue to evolve, the necessity for robust security awareness becomes increasingly urgent.

Security culture refers to the set of values, beliefs, and behaviors that determine how an organization approaches cybersecurity. It involves educating employees about potential risks and equipping them with the skills to recognize and respond to security incidents effectively. A strong security culture ensures that all members of the organization prioritize security in their daily activities and decision-making processes.

Importance of Security Culture:

- Mitigation of Human Error: With 90% of security breaches occurring due to human error, fostering a robust security culture is crucial[2]. It empowers employees to recognize and respond to threats effectively, reducing the likelihood of incidents.
- Enhanced Compliance: A strong security culture supports adherence to regulatory requirements and industry standards, minimizing the risk of legal penalties.
- Reputation Protection: By prioritizing security, organizations can safeguard their reputation and maintain customer trust, even in the face of potential cyber threats.

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. Research indicates that 80% of organizations[3] reported a reduction in phishing susceptibility following security awareness training. Regular training can reduce risk from 60% to 10% within the first 12 months[4], and companies that consistently engage in these programs have seen a 70% reduction in security incidents[5]. These statistics underscore the effectiveness of well-implemented security awareness training programs in enhancing organizational resilience against cyber threats.

“

70%

Cyber security awareness training leads to a 70% reduction in security-related risks

Key elements of security awareness training

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:** Best practices for safely using public Wi-Fi and securing remote work environments are emphasized.

Recognizing threats

- **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.

Best practices

- **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 procedures

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

Risk management

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

Incident response

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

Ongoing training and awareness

- 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].

Return on Investment (ROI)

Investing in security awareness training yields significant returns. On average, such programs can deliver a 37-fold return on investment, with even the least effective programs offering a 7-fold ROI[4]. Smaller businesses can achieve an ROI of 69%, while larger companies can see returns as high as 562%[6]. These figures highlight the financial benefits of investing in robust security training initiatives, which not only reduce risk but also contribute to cost savings and improved business outcomes.

Having established a solid foundation in training, we now turn our attention to understanding the current cybersecurity threat landscape. This context highlights why continuous education is vital in adapting to new challenges.

Current cybersecurity threat landscape

The cybersecurity landscape is characterized by sophisticated threats such as phishing, ransomware, and social engineering attacks. Understanding these threats is crucial for developing effective training programs and building a resilient security culture.

Human Error and Non-Malicious Actions

Human error continues to be a major factor in cybersecurity incidents. According to the Verizon 2024 Data Breach Investigations Report, 68% of breaches in 2023 involved a non-malicious human element[1]. This statistic highlights the critical role of employee awareness in preventing data breaches. In fact, 90% of security breaches[2] occur due to human error, underscoring the need for comprehensive security awareness programs to mitigate human-related vulnerabilities.

Prevalent Threats

Phishing remains a prevalent threat, affecting **84% of businesses[3]**. The rapid pace at which phishing attacks can deceive employees—often in **less than 60 seconds**—demonstrates the critical need for quick detection and response skills.
Social engineering attacks, particularly Business Email Compromise (BEC) and CEO Fraud, are increasingly common. **Over 40%** of successful social engineering attacks were BEC or CEO Fraud[1], emphasizing the need for targeted training on these specific threats:

- **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

The UK government's Cyber Security Breaches Survey 2024 found that 80%[3] of organizations reported a reduction in phishing susceptibility following security awareness training. This data highlights the importance of training employees to recognize and respond to phishing attempts effectively.

68% of breaches in 2023 involved a non-malicious human element.

Business Implications

A lack of security awareness can lead to severe business implications, including financial losses, reputational damage, and regulatory penalties. The IBM Cost of a Data Breach Report 2023 revealed that organizations with a high level of security skills shortage faced an average data breach cost significantly higher than the industry average.

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.

Challenges in driving security awareness

Despite its benefits, implementing effective security awareness training presents challenges. Approximately **45% of employees** report receiving no security training from their employers, and only **52% of organizations** conduct anti-phishing training, with just 30% offering ransomware-focused security training.

Furthermore, 62% of companies lack adequate training to reap significant benefits[5]. Addressing these gaps is crucial for organizations aiming to build a comprehensive security culture.

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:

- Limited resources for training programs
- Difficulty measuring effectiveness
- Keeping up with evolving threats requires continuous updates
- Employee resistance due to perceived low priority or inconvenience
- Insufficient participation
- Resource constraints (only 7.5% provide adaptive training based on regular test results)
- Ongoing education necessary as cyber threats evolve

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

45% of employees report receiving no security training from their employer

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.

80% of organizations reported a reduction in phishing susceptibility following security awareness

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 management risk 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

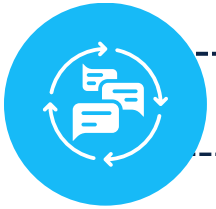
6. Gamification

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. Employees begin to forget their training after four months, making regular awareness sessions essential to maintain vigilance. Phishing awareness training has been shown to reduce the likelihood of clicking on phishing links by 30%, with a 40% improvement in overall phishing awareness. These improvements emphasize the importance of maintaining consistent and engaging training programs to ensure long-term effectiveness.

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

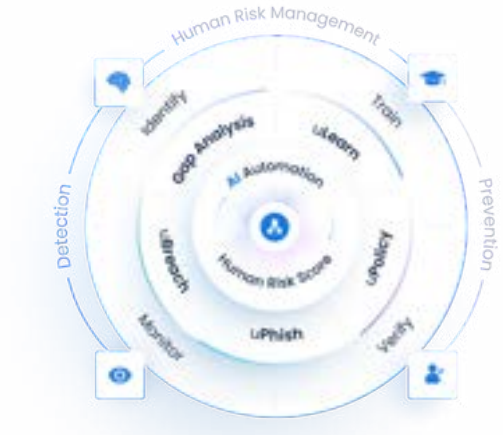
Ensuring continuous improvement in security awareness programs is essential for maintaining their effectiveness over time.

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. While 84% of programs aim to bring about measurable changes in employee behavior, only 43% consistently track these changes. Regular updates to training materials and incorporating behavioral analytics are essential for ensuring that programs remain relevant and effective in addressing emerging threats.



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 is a proven strategy for reducing human error, which continues to be a significant factor in cybersecurity breaches. This white paper has demonstrated how targeted, continuous training not only mitigates risk but also aligns organizations with essential cybersecurity regulations. By implementing comprehensive training programs, leveraging engaging techniques like gamification, and fostering a security-conscious environment, organizations can significantly reduce their vulnerability to cyber threats. The potential 37-fold return on investment underscores the financial wisdom of prioritizing security awareness.

However, building this culture requires more than just periodic training sessions. It demands ongoing commitment, from the C-suite to entry-level employees. Every member of the organization must understand their role in maintaining cybersecurity and feel empowered to act on this responsibility.

The time to act is now. With cyber threats evolving rapidly, organizations cannot afford to delay in strengthening their human firewall. By taking immediate steps to enhance security awareness, companies can protect their assets, reputation, and bottom line while contributing to a safer digital ecosystem for all.

Key takeaways:

Human Element in Breaches: With 68% of breaches involving a non-malicious human element, comprehensive security awareness training is essential to mitigate these vulnerabilities.

Targeted Training Needs: Over 40% of successful social engineering attacks are Business Email Compromise (BEC) or CEO Fraud, underscoring the need for targeted training to combat these specific threats.

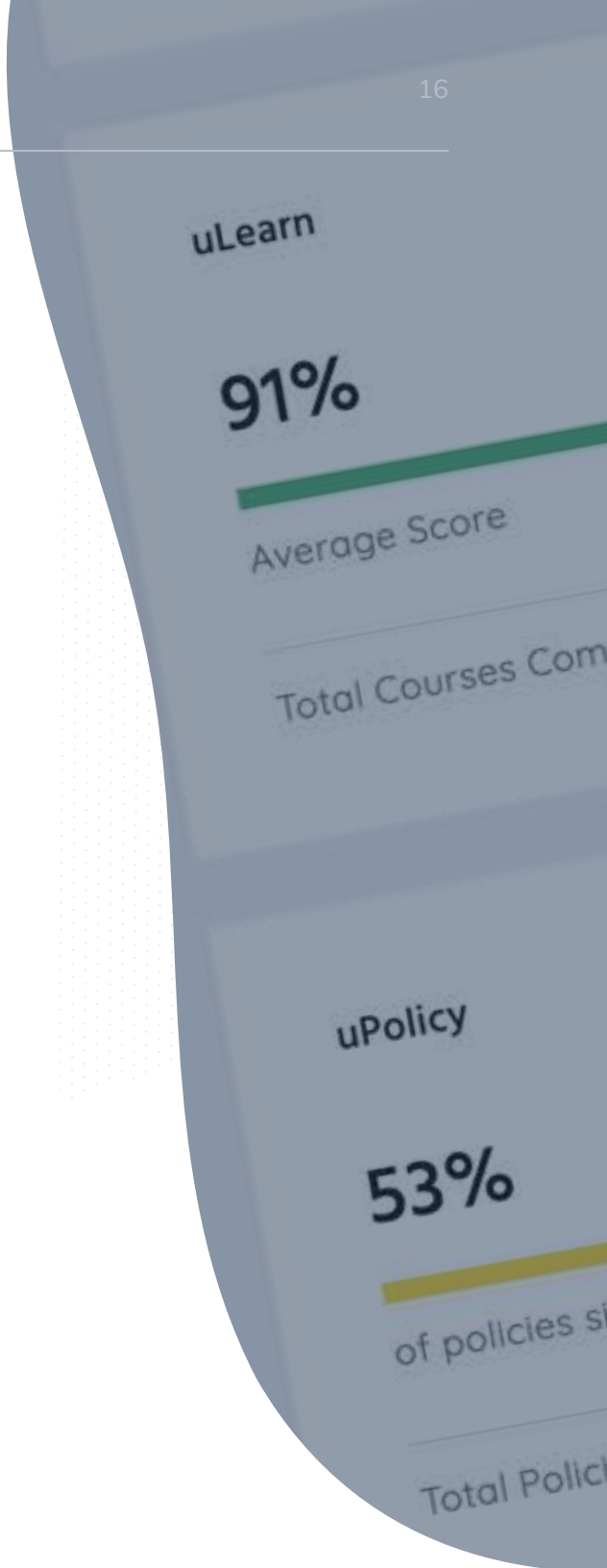
Effectiveness of Training Programs: 80% of organizations reported a reduction in phishing susceptibility following security awareness training, demonstrating its effectiveness in enhancing cybersecurity resilience.

Leadership and Culture: Engaging leadership and embedding security into company culture fosters a top-down approach that values security at all organizational levels.
Technology Solutions: Leveraging platforms like usecure allows for customized training that meets diverse business needs, enhancing overall cybersecurity posture.

Risk Reduction and Trust Building: Prioritizing security awareness reduces the risk of data breaches and strengthens trust with clients and stakeholders.

Continuous Improvement: Regular updates to training materials and soliciting employee feedback ensure that programs remain relevant and effective in addressing emerging threats.

> 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 2024 Data Breach Investigations Report (DBIR): 1
2. IBM (2024) Cost of a Data Breach Report: 2
3. UK Government's Cyber Security Breaches Survey 2024:
4. Ponemon Institute:
5. Keepnet Labs:
6. Osterman Research
7. usecure Case Study: Winning Group achieves a 90% reduction in phishing risk within 6 months.

usecure