TRUSTYCYBER

Business Case Paper

From Checkboxes to Culture: Closing the Cybersecurity Behaviour Gap through Gamification

Executive Summary

Organisations increasingly understand that robust Governance, Risk, and Compliance (GRC) programs are essential for managing cybersecurity risks. However, strong policies and frameworks alone do not guarantee sustained, secure behaviours across an organisation—particularly during periods of rapid growth, organisational change, or hybrid working environments.

This white paper explores the persistent behavioural gap between traditional cybersecurity training approaches and the need for deeply embedded, continuously reinforced security practices. Drawing inspiration from personal experiences with incentivised health monitoring, we propose gamification as a scientifically grounded, transformative strategy for achieving enduring, proactive cybersecurity behaviours across diverse organisational contexts.

The Behavioural Gap in Cybersecurity

As organisations scale, mature, or adopt new technologies, maintaining effective cybersecurity behaviours becomes increasingly difficult. While strong GRC foundations—such as risk assessments, vulnerability scanning, and policy enforcement—are essential, they can be undermined when execution relies solely on a small, centralized security team.

During periods of high growth this tension is revealed: whilst governance structures may be sound, behavioural consistency across departments and teams begins to weaken. This is not necessarily due to a lack of intent or awareness, but rather a structural inability to scale security behaviours across growing, distributed workforces.

Studies in organisational psychology consistently show that behavioural drift occurs when reinforcement is absent, particularly when training is limited to passive, one-time formats. Employees often forget, deprioritise, or sidestep security procedures in favour of productivity—especially under stress or deadline pressure.

Without mechanisms for continuous reinforcement and recognition, even well-designed policies are at risk of being left behind.

Personal Inspiration: Health Gamification

The concept of gamified cybersecurity emerged for me from a personal health journey. Following a minor health scare, I began using a smart watch to track exercise, sleep, and cardiovascular activity. To my surprise, my health insurer not only supported this practice but incentivised it—offering rebates and rewards in exchange for reaching activity thresholds. Over time, the combination of tracking, real-time feedback, and

achievable goals reshaped my daily habits. I exercise more regularly, pay closer attention to recovery, and have become measurably healthier.

What stood out was not just the personal improvement, but the insight that these small, reinforced behaviours reduced risk at scale—benefitting both me and my insurer. This led to a pivotal question: could the same behavioural reinforcement model be applied to cybersecurity in the workplace? Could organisations reduce risk by encouraging incremental, measurable security actions in a way that felt engaging and rewarding?

The Limits of Traditional Awareness Training

Most organisations still rely heavily on security awareness training, phishing simulations, and annual compliance refreshers to improve cybersecurity posture. However, research shows these approaches have limited efficacy. According to the previous SANS security awareness reports, only 20–30% of employees retain key messages from awareness training after 30 days. The Verizon Data Breach Investigations Report often cites human error as a factor in over 80% of breaches, despite widespread training initiatives.

Training often fails because it is narrowly focused, infrequent, and delivered in a way that feels disconnected from daily responsibilities. The content typically centres on phishing and password security while ignoring the broader spectrum of security behaviours. Without continuous reinforcement, feedback, a sense of ownership, and incentives these initiatives fail to achieve meaningful and lasting change.

The Success of Gamification in Other Sectors

Gamification has demonstrated proven benefits in sectors like health, education, fitness, and workplace productivity. In healthcare, gamified interventions have led to measurable improvements in behaviour. A large study of a fitness app found that during step-tracking competitions, users increased their physical activity by 23% on average. Similarly, a systematic review of health gamification studies reported that 59% of trials showed positive outcomes, particularly for encouraging physical activity.

In education, gamified learning has been linked to higher engagement and performance. Meta-analyses show significant improvements in students' cognitive skills, motivation, and classroom participation. In practice, this translates to higher quiz scores, better concept retention, and increased voluntary practice when game mechanics are (respectfully) integrated into curricula. In the workplace, surveys indicate that employees support gamified systems.

Gamification in Cybersecurity Today

Currently, the use of gamification in cybersecurity is concentrated in awareness training and phishing simulations. Organisations have begun to implement game-like elements such as interactive quizzes, scenario-based challenges, and badges for completion. Some companies have introduced cybersecurity-themed escape room exercises that turn abstract security policies into hands-on challenges. These initiatives often lead to higher knowledge retention and greater enthusiasm among employees.

Phishing simulation platforms also incorporate gamified elements. Instead of merely testing employees with fake phishing emails, programs now award points or rewards for spotting and reporting malicious messages. This approach transforms phishing tests into collaborative challenges, increasing participation and vigilance. Studies show that gamified phishing simulations can boost detection rates by over 50%.

Despite these successes, gamification remains underutilised in cybersecurity overall, usually limited to awareness and training contexts. Gartner surveys on security awareness programs found that only about 30% of organisations use gamified training techniques. Traditional methods such as slide decks and video modules still dominate. This highlights an opportunity to expand gamification beyond basic training into continuous reinforcement of security behaviours.

Behavioural Psychology: Why Gamification Works

Gamification's effectiveness is grounded in behavioural psychology. One of the key principles is positive reinforcement, where immediate rewards strengthen the likelihood of repeated behaviour. In cybersecurity, rewards such as points or badges for reporting phishing emails serve this purpose, encouraging repetition of secure behaviours.

Another core principle is the use of feedback loops. Effective gamification provides continuous feedback, allowing individuals to see the results of their actions and adjust accordingly. For example, real-time dashboards that reflect successful phishing reports offer validation and maintain user engagement.

Habit formation through repetition is also central to gamification. Small, consistent rewards given over time help transform one-time behaviours into sustained habits. Studies show that spaced micro-learning with gamified elements improves knowledge retention significantly. By encouraging frequent engagement through brief, rewarding tasks, organisations can embed security practices into daily routines.

Goal setting and achievement further enhance the effectiveness of gamification. Games provide users with clear goals and a sense of progression, which are known to boost motivation and persistence. Visual elements such as progress bars and levels

help break down long-term objectives into manageable steps, reinforcing a sense of accomplishment.

Together, these principles align with intrinsic human motivators, making secure behaviour feel personally rewarding. Over time, this approach can reshape organisational security culture by turning individual improvements into collective norms.

Quantifying the ROI of Gamification

Cybersecurity gamification offers tangible financial benefits. For instance, in an organisation with 250 employees and an average breach cost of $4,500, a 30% reduction in incidents through gamified interventions could save over $337,000 annually. This figure does not account for the additional soft benefits such as improved audit readiness, stakeholder trust, and reduced pressure on security teams.

Recent studies further support this potential. Research by Ponemon Institute found that organisations incorporating peer competition and team games into their training saw a 46% improvement in security culture. These findings underscore that changing user behaviour can have a direct impact on breach prevention and associated costs. Gamification, by improving engagement and reinforcing secure behaviour, contributes significantly to this outcome.

Implementing Gamification Effectively

Implementing gamification begins with identifying the key behaviours that align with organisational risk posture and compliance goals. These behaviours should be specific and measurable. Organisations should then develop a reward system that combines intrinsic and extrinsic motivators, such as recognition and tangible rewards.

Tracking and reporting should be automated where possible, using data from existing tools Learning Management Systems. Progress should be made visible through dashboards and leaderboards, creating shared accountability and engagement. Regular analysis of participation and outcomes ensures the program remains aligned with security objectives and continues to evolve.

Gamification should be seen as a continuous process, not a one-time intervention. By embedding it into regular workflows and maintaining consistent feedback, organisations can create a lasting impact on security behaviour.

Conclusion: From Compliance to Culture

Gamification represents more than a new training method—it signals a shift in how organisations think about cybersecurity culture. It moves the conversation from "what must we do to comply?" to "what can we do to empower secure behaviour?"

By treating cybersecurity like a shared responsibility, reinforcing positive actions, and making participation visible and rewarding, organisations can reduce risk while building a more engaged, resilient workforce. The parallel with health tracking is instructive. Just as real-time feedback and small habit changes have transformed personal wellness, they can do the same for cybersecurity.

Through gamification, cybersecurity becomes something employees want to participate in—not just something they're told to do. That's the foundation of culture. And that's the future of cyber resilience.

About **TRUSTY**CYBER

TRUSTYCYBER was founded to close the gap between cybersecurity frameworks and sustained behavioural change—combining industry-aligned coaching with gamified software that makes secure behaviours visible, measurable, and rewarding.

Our flagship platform, TRUSTYAPP, empowers organisations to embed critical security behaviours into everyday workflows through points, badges, leaderboards, and behavioural nudges. From reporting phishing attempts and completing training to contributing to risk identification and team leadership, TRUSTYAPP tracks and rewards real actions aligned to your security program.

Backed by behavioural science and designed for ease of use, TRUSTYAPP integrates seamlessly with existing tools and frameworks. Whether you're looking to enhance engagement, reduce incidents, or reinforce a positive security culture, TRUSTYAPP provides the structure, incentives, and insights needed to scale secure behaviours across your organisation.

For teams working towards compliance with standards like ISO/IEC 27001, TRUSTYCYBER also offers cohort-based coaching. This structured, expert-led approach helps organisations build, implement, and maintain an Information Security Management System (ISMS) that is both audit-ready and culture-aware.

By combining gamified reinforcement with practical coaching, TRUSTYCYBER supports a transition from reactive training to proactive security culture—helping organisations not only meet their compliance goals but create long-term resilience through empowered people.

To learn more or request a demo, visit www.trustycyber.com