CYBER REBELS

Beyond Awareness

Why Cybersecurity Training Must Become Behaviour-Led

A Framework for Human-Centred Cybersecurity Using the Cyber Rebels Five-Domain Model

DOI: 10.5281/ZENODO.19053824

BEYOND AWARENESS

WHY CYBERSECURITY TRAINING MUST BECOME BEHAVIOUR-LED

A FRAMEWORK FOR HUMAN-CENTRED CYBERSECURITY USING THE CYBER REBELS FIVE-DOMAIN MODEL

AUTHOR: ANDY LONGHURST

ORGANISATION: CYBER REBELS

FIRST PUBLISHED DATE: 15 MARCH 2026

Executive Summary

Cybersecurity has become a routine concern for organisations of all sizes. Ransomware attacks, data breaches, and online fraud are now widely reported, and most employees understand that cyber criminals frequently target businesses through phishing emails, fraudulent communications, and other forms of social engineering.

In response, many organisations have implemented cybersecurity awareness training programmes designed to help employees recognise threats and follow security policies when interacting with digital systems. These programmes typically explain how attacks work, show examples of malicious messages, and encourage employees to remain vigilant when responding to unexpected requests.

The underlying assumption behind this approach has been straightforward: if employees are aware of cyber threats, they will avoid them.

However, real-world experience has increasingly shown that awareness alone does not consistently prevent cyber incidents. Phishing attacks continue to succeed, fraudulent requests are sometimes approved, and sensitive information is occasionally shared in response to convincing communications. In many cases, the individuals involved had already completed cybersecurity awareness training and were familiar with the risks.
This suggests that the challenge organisations face is not simply a lack of knowledge.

Cyber incidents frequently occur during normal business activity, when employees must make rapid decisions while managing busy workloads, responding to colleagues, or dealing with urgent requests. Attackers deliberately design their communications to exploit these everyday working conditions, blending malicious messages into legitimate workflows and

manipulating the decision-making processes employees rely on to perform their jobs.

Under these circumstances, cybersecurity failures are often behavioural rather than informational. Employees may understand cyber threats in theory, yet still make unsafe decisions when confronted with realistic and ambiguous situations.

This paper argues that improving organisational cybersecurity therefore requires a shift in how cybersecurity training is designed.

Rather than focusing primarily on increasing awareness of cyber threats, organisations must develop the behavioural capabilities employees rely on when making decisions in real working environments. These capabilities include recognising contextual risk, verifying unusual requests, maintaining secure operational habits, and escalating suspicious activity when something appears wrong.

To support this shift, the paper introduces the Cyber Rebels Five-Domain Model, a behaviour-focused framework designed to strengthen cybersecurity decision-making across the workforce. The model identifies five key areas of behavioural capability that underpin secure organisational behaviour:

- Contextual Risk Recognition
- Verification and Control Discipline
- Secure Operational Behaviour
- Incident Judgement and Escalation
- Professional Cyber Judgement

Together, these domains provide a structured approach to developing the judgement, habits, and professional responsibility required to manage cyber risk in everyday organisational environments.

By examining the limitations of traditional awareness training and exploring how attackers exploit human behaviour, this paper demonstrates why behaviour-led cybersecurity training represents a critical next step in organisational cyber resilience.

Organisations that strengthen the behavioural dimension of cybersecurity will be significantly better positioned to detect, disrupt, and respond to modern cyber threats.

1. The Promise of Cybersecurity Awareness Training

Over the past two decades, cybersecurity awareness training has become one of the most widely adopted strategies for addressing human-related cyber risk. As organisations increasingly recognised that employees could unintentionally expose systems and data to attack, training programmes were introduced to educate staff about common threats such as phishing emails, malicious

attachments, password misuse, and social engineering
.
Regulators and industry frameworks reinforced this approach. Standards such as ISO 27001, the NIST Cybersecurity Framework, and the UK government's Cyber Essentials scheme all emphasise the importance of security awareness programmes as part of a comprehensive cybersecurity strategy. In many sectors, organisations are expected to demonstrate that employees receive regular training and understand their responsibilities when handling sensitive systems or information.

As a result, awareness training became embedded within organisational security practices across both public and private sectors.

At its core, cybersecurity awareness training was built on a simple and compelling promise: that improving employees' understanding of cyber threats would reduce the likelihood of successful attacks.

The assumption was that if employees could recognise common attack techniques—such as phishing emails, fraudulent requests, or suspicious links—they would be less likely to fall victim to them. By increasing knowledge of cyber risks and reinforcing organisational security policies, awareness programmes aimed to encourage safer behaviour across the workforce.

Typically, these programmes involve annual or periodic training modules that introduce employees to common cyber threats and organisational policies. Employees may be shown examples of phishing emails, taught how to create stronger passwords, and reminded of procedures for reporting suspicious activity. Many organisations also run simulated phishing campaigns to test whether employees can recognise malicious messages.

The intention behind these initiatives is clear and well-founded.

Human behaviour has long been recognised as an important factor in cybersecurity incidents. According to Verizon's Data Breach Investigations Report, the human element is present in the majority of breaches, often through phishing, credential misuse, or social engineering. Security awareness training was therefore introduced to reduce these risks by improving employees' understanding of cyber threats and encouraging safer behaviour
.
In principle, the logic appears sound. If employees understand how cyber attacks work, recognise the warning signs of malicious activity, and follow established security policies, the likelihood of successful attacks should decrease.

In many respects, awareness training has achieved part of this objective. Across most organisations today, employees are significantly more familiar with common cyber threats than they were a decade ago. Terms such as phishing, ransomware, and social engineering are now widely recognised, and most employees understand the importance of basic practices such as strong passwords and reporting suspicious communications.

For many organisations, awareness training therefore represents a practical and scalable way to address human-related cyber risk. It allows organisations to demonstrate regulatory compliance, communicate security expectations to employees, and establish a shared understanding of cybersecurity responsibilities across the workforce.

However, while awareness training has successfully increased knowledge about cybersecurity threats, the persistence of human-enabled breaches suggests that knowledge alone may not be sufficient to change behaviour
.
If employees already understand what cyber threats look like, why do attacks that rely on human interaction continue to succeed?

2. The Reality: Breaches Continue Despite Training

Despite the widespread adoption of cybersecurity awareness programmes, cyber incidents involving human behaviour remain extremely common.

Over the past decade, organisations across the public and private sectors have invested significant time and resources into cybersecurity education. Employees regularly complete online awareness modules, participate in simulated phishing campaigns, and acknowledge organisational security policies. In many organisations, these programmes are now embedded into annual compliance cycles and onboarding processes.

However, the continued frequency of cyber incidents suggests that awareness training alone has not solved the human element of cybersecurity risk.

Data from the UK Government's Cyber Security Breaches Survey illustrates the scale of the problem. The 2025 survey found that 43% of UK businesses and 30% of charities experienced a cybersecurity breach or attack in the previous 12 months. Among organisations that identified an attack, phishing was by far the most common threat, affecting approximately 84% of those businesses.

These figures demonstrate that cyber attacks targeting employees remain widespread despite the routine use of cybersecurity awareness training.

Industry research also consistently highlights the central role that human behaviour plays in successful cyber attacks. Various studies estimate that between 88% and 95% of breaches involve some form of human interaction or error, including actions such as responding to phishing emails, reusing compromised credentials, or approving fraudulent requests.

This does not necessarily indicate that employees lack awareness of cyber threats. In many cases, individuals involved in incidents have already received training and understand the security policies designed to protect their organisation.

Yet breaches still occur.

Recent high-profile cyber incidents in the United Kingdom illustrate how attackers continue to exploit human behaviour rather than purely technical vulnerabilities
.
In 2025, Marks & Spencer experienced a major cyberattack that disrupted online operations and forced the retailer to suspend digital ordering systems while investigations and recovery efforts were underway. The incident resulted in significant operational disruption and highlighted the growing impact of cyber attacks on major organisations. Investigations suggested that attackers used social engineering techniques to gain access to systems before deploying ransomware, demonstrating how human interaction can act as the initial entry point for sophisticated attacks.

Large enterprises are not the only organisations affected. A widely cited example within the UK logistics sector involved Knights of Old, a Northamptonshire-based transport company that collapsed following a ransomware attack in 2023. The breach reportedly originated from a single compromised employee password, which allowed attackers to gain access to internal systems. The resulting disruption to operations ultimately forced the company into administration, leading to the loss of hundreds of jobs.

These incidents illustrate a critical pattern within modern cyber attacks. Attackers rarely need to defeat advanced security technologies if they can manipulate human behaviour.

Phishing emails, fraudulent messages, and social engineering attacks are specifically designed to exploit human decision-making. They create urgency, impersonate authority figures, or mimic legitimate operational requests in order to encourage employees to act quickly
.
Under these conditions, employees may make decisions that contradict what they learned during cybersecurity training
.
This does not mean employees are careless or negligent. Rather, it reflects the reality that decision-making in operational environments is influenced by factors such as time pressure, workload, organisational culture, and competing priorities.
As a result, employees who understand cybersecurity risks may still make unsafe decisions in the moment.

This pattern highlights a fundamental limitation of traditional cybersecurity awareness training. Increasing knowledge about cyber threats does not automatically translate into secure behaviour when individuals are faced with real-world situations that involve urgency, ambiguity, and operational pressure.

To understand why this gap exists, it is necessary to examine how employees actually make decisions within their daily work environments.

3. The Core Problem: Cybersecurity Is Not a Knowledge Problem

Traditional cybersecurity awareness training is built on a simple assumption: if

employees understand cyber risks and know the correct security procedures, they will behave securely when faced with a threat.

This assumption appears logical. Education has long been used to change behaviour in many areas of organisational life, from health and safety to regulatory compliance. By increasing knowledge and reinforcing policies, organisations expect individuals to adopt safer practices.

However, the reality of cybersecurity decision-making is far more complex.

Knowing the correct behaviour does not necessarily mean that behaviour will occur in practice. Human decision-making is influenced by a wide range of behavioural factors that operate in real time, often under conditions that differ significantly from the controlled environments in which training takes place.

Employees rarely encounter cyber threats in calm, clearly labelled situations. Instead, they experience them in the middle of normal working activity. Emails arrive while staff are handling multiple tasks. Requests appear within busy communication channels. Messages often resemble legitimate operational instructions from colleagues, suppliers, or senior managers.

Under these conditions, individuals must make rapid decisions with limited time to evaluate the situation.

Cyber attackers understand this dynamic extremely well.

Modern social engineering attacks are specifically designed to exploit human cognitive shortcuts and workplace pressures. Rather than relying solely on technical exploitation, attackers manipulate urgency, authority, and trust in order to influence behaviour.

A phishing message may claim that a payment must be processed immediately to avoid disruption to a supplier. A fraudulent email may appear to come from a senior executive requesting confidential information. A malicious link may be embedded within what appears to be a routine system notification.

In each case, the attack attempts to trigger a rapid behavioural response before the recipient has time to question the legitimacy of the request.

These techniques exploit fundamental aspects of human psychology. People tend to respond quickly to authority figures, prioritise urgent requests, and rely on familiar patterns when interpreting information. In a busy work environment, these instincts can override the more deliberate reasoning processes that cybersecurity training attempts to promote.

Operational context further amplifies this challenge.

Employees are often evaluated based on efficiency, responsiveness, and productivity. They may feel pressure to resolve requests quickly or avoid delaying

colleagues and clients. Security checks that appear to slow down work can therefore be perceived as obstacles rather than protective controls.

As a result, individuals may bypass verification steps or act on incomplete information in order to maintain workflow momentum.

These behaviours are not necessarily the result of negligence. In many cases they represent rational decisions made within the context of competing organisational priorities.

The problem, therefore, is not that employees are unaware of cyber threats. In many organisations, staff can correctly identify phishing emails in training exercises and demonstrate knowledge of security policies.

The challenge arises when individuals must apply that knowledge in complex, ambiguous situations where multiple behavioural pressures are operating simultaneously.

In these moments, knowledge alone is rarely sufficient.

Employees must be able to recognise when a situation presents cyber risk, pause long enough to evaluate the request, apply verification practices consistently, and escalate concerns when necessary. These actions require behavioural capability rather than simple awareness.

Traditional awareness training often fails to develop these capabilities because it focuses primarily on information delivery. Employees are taught what threats look like, but they are rarely trained to navigate the behavioural conditions under which those threats appear

.

As a result, organisations may succeed in increasing cybersecurity knowledge without significantly improving real-world security behaviour.

This gap between knowledge and behaviour represents one of the most important challenges in modern cybersecurity strategy.

If organisations wish to reduce the human component of cyber risk, training programmes must evolve beyond awareness and begin focusing on the behavioural skills required to make secure decisions in real operational environments.

4. The Gap in Current Cybersecurity Training

One of the most significant weaknesses in traditional cybersecurity awareness programmes lies not only in how training is delivered, but also in how success is measured.

In many organisations, the effectiveness of cybersecurity training is evaluated using relatively simple indicators. Security teams track metrics such as training

completion rates, quiz scores, and employee acknowledgement of organisational policies. If employees complete their annual training modules and pass knowledge-based assessments, the programme is often considered successful from a governance or compliance perspective.

These metrics are useful for demonstrating that training has been delivered. However, they reveal very little about how employees actually behave when confronted with a real cyber threat.

For example, many organisations conduct phishing simulation exercises to test whether employees can recognise suspicious emails. These simulations typically measure whether a user clicks a malicious link or reports the email to the security team. While these tests can provide useful insights, they also illustrate the limitations of awareness-based training.

In a simulated environment, employees often have time to carefully analyse the message and recall the training they previously completed. However, real phishing attacks rarely occur under these conditions. They arrive during busy workdays, mixed in with legitimate emails, and often contain elements specifically designed to trigger urgency or authority. In these real-world situations, the behavioural pressures that influence decision-making are far stronger than those present in controlled testing environments.

Research into phishing simulations reflects this challenge. Many organisations observe initial improvements in phishing detection immediately after training campaigns, only for employee click rates to gradually increase again over time. This pattern suggests that awareness gained during training may not translate into long-term behavioural change.

Similarly, high completion rates for awareness training modules can create the impression that the workforce is well prepared to handle cyber threats. In reality, these programmes often rely on passive learning formats such as slide-based presentations or short video courses, followed by simple multiple-choice assessments.

Employees may successfully answer questions about phishing indicators or password policies, yet still struggle to apply this knowledge in real operational situations. Knowing that suspicious emails often contain unusual requests does not necessarily help an employee evaluate a convincing message that appears to come from a trusted colleague.

Another indicator of this gap can be seen in incident reporting behaviour. Many organisations encourage employees to report suspicious activity, yet internal security teams frequently observe underreporting of potential incidents. Employees may hesitate to escalate concerns because they are unsure whether something truly represents a threat, or because they fear raising a false alarm. This reluctance highlights a behavioural barrier that traditional awareness programmes rarely address. Employees may understand that reporting incidents is important, but they may lack the confidence or judgement required to identify when escalation is appropriate.

The result is a paradox within many organisations. Security training metrics may indicate that employees are well informed about cyber risks, while operational evidence suggests that unsafe decisions and missed warning signs continue to occur.

In other words, organisations are often measuring knowledge rather than behaviour.

This distinction is critical. Knowledge-based metrics provide reassurance that training programmes have been delivered and understood. However, they do not necessarily reflect whether employees have developed the behavioural capabilities required to recognise risk, verify suspicious requests, and respond appropriately to potential cyber incidents.

Until organisations begin measuring and developing real security behaviour, this gap between training outcomes and operational reality is likely to persist.
Recognising this gap is the first step toward developing a more effective approach to cybersecurity training.

5. The Shift Toward Behaviour-Led Cybersecurity Training

As organisations increasingly recognise the limitations of traditional awareness programmes, a shift is beginning to emerge within the cybersecurity industry. Rather than focusing solely on increasing employee knowledge, security leaders are starting to examine how individuals actually behave when faced with cyber risk.

This shift reflects a broader understanding that cybersecurity is fundamentally a human decision-making challenge as much as it is a technical one. While technologies such as firewalls, endpoint protection systems, and identity management tools play a critical role in protecting digital infrastructure, the actions taken by employees often determine whether a threat is successfully stopped or allowed to progress.

Attackers understand this dynamic and have adapted their strategies accordingly. Modern cyber attacks increasingly rely on social engineering techniques that exploit human behaviour rather than attempting to bypass technical controls directly. By manipulating urgency, authority, curiosity, or trust, attackers can influence individuals to take actions that inadvertently open the door to compromise.

Recent advances in artificial intelligence are accelerating this trend. AI tools now allow attackers to generate highly convincing phishing emails, realistic fake websites, and impersonation messages that closely resemble legitimate business communications. What once required significant time and technical skill can now be produced in seconds.

Emails can be generated that perfectly mimic a company's tone of voice, branding, and internal communication style. Fraudulent websites can replicate legitimate login pages with near-perfect accuracy. Even simple reconnaissance tasks — such

publicly available information about employees, suppliers, or organisational structures — can now be automated at scale.

As a result, the distinction between legitimate communication and malicious deception is becoming increasingly difficult for employees to identify based on appearance alone.

This development further exposes the limitations of traditional awareness-based training. Teaching employees to look for obvious warning signs such as poor grammar, unusual formatting, or suspicious domain names is no longer sufficient when attackers can produce messages that appear indistinguishable from legitimate communications.

In this environment, effective cybersecurity behaviour relies less on recognising obvious indicators of attack and more on applying disciplined verification practices and sound judgement before taking action.

Behaviour-Led Cybersecurity Training addresses this challenge by focusing on the behavioural capabilities that allow employees to operate securely even when attacks appear convincing.

Instead of relying solely on awareness of threat indicators, behaviour-led training develops the habits and decision-making processes that encourage employees to pause, question unexpected requests, verify identities, and escalate concerns when something appears unusual.

In practical terms, this approach focuses on strengthening the behavioural skills that shape how employees respond to potentially risky situations within their daily work.

This shift also aligns with a broader movement within cybersecurity strategy toward human-centred security design. Rather than assuming that employees will always behave perfectly if given the correct instructions, organisations are increasingly recognising the need to design systems, processes, and training around realistic human behaviour.

Behaviour-Led Cybersecurity Training represents a natural extension of this philosophy. Instead of relying on awareness alone, organisations focus on developing behavioural resilience across the workforce.

Employees learn not only what cyber threats look like, but how to recognise risky situations, pause before acting, and apply verification habits consistently within their daily workflows.

Over time, these behaviours become embedded within organisational culture, strengthening the human layer of cybersecurity defence.

To support this shift, organisations require a structured framework that defines the behavioural capabilities needed for secure decision-making.

The Cyber Rebels Five-Domain Model was developed to provide exactly this structure, identifying the key areas of behavioural competence that organisations must cultivate in order to build a resilient cybersecurity culture.

6. The Cyber Rebels Five-Domain Model

If cybersecurity failures are primarily behavioural failures rather than knowledge failures, then improving organisational resilience requires a framework that focuses specifically on how employees recognise risk, make decisions, and respond to unusual situations.

To address this challenge, Cyber Rebels developed the Five-Domain Model, a behavioural framework designed to strengthen the human layer of cybersecurity defence. Rather than focusing solely on awareness of threats, the model identifies the practical behavioural capabilities employees must develop in order to operate securely within modern work environments.

Each domain represents a critical component of secure decision-making. Together, the five domains create a structured approach to developing behavioural cybersecurity capability across an organisation.

Importantly, the model does not treat employees as the "weakest link" in security. Instead, it recognises that with the right training and organisational culture, employees can become a highly effective layer of cyber defence.

Contextual Risk Recognition

The first domain focuses on an employee's ability to recognise when a situation may involve cyber risk.

Many cyber attacks succeed because malicious activity is disguised within normal business operations. Phishing emails often resemble legitimate communications, and fraudulent requests frequently appear to come from trusted colleagues, suppliers, or system notifications. If employees do not recognise that a situation might involve cyber risk, they are unlikely to apply the caution or verification steps necessary to prevent compromise.

Contextual Risk Recognition therefore focuses on developing the ability to interpret the surrounding circumstances of a request rather than relying solely on obvious technical indicators.

For example, an employee in the finance department may receive an urgent email requesting a change to supplier payment details. The message appears legitimate and contains correct company branding. Traditional awareness training might encourage the employee to look for suspicious formatting or spelling errors. However, a behaviour-led approach encourages the employee to consider the broader context of the request.

Is this type of request normally made through email?

Does the request match the organisation's normal financial processes?
Is there unusual urgency associated with the message?

By recognising that the situation itself represents potential risk, the employee becomes more likely to apply verification procedures before taking action.

Developing this contextual awareness significantly reduces the likelihood that employees will treat suspicious activity as routine business communication.

Verification & Control Discipline

Once risk is recognised, the next critical behaviour is verification.

Verification & Control Discipline focuses on developing consistent habits around confirming requests before acting on them. Many successful cyber attacks rely on bypassing verification processes by creating urgency or exploiting trust relationships within organisations.

For example, attackers conducting business email compromise attacks often impersonate senior executives or trusted suppliers. The message may instruct an employee to process a payment quickly or share sensitive information. If the recipient acts immediately, the attack succeeds.

Verification discipline encourages employees to pause and confirm the legitimacy of the request through independent channels. This might involve calling a colleague directly, confirming instructions through a separate communication system, or following established organisational procedures for authorising financial transactions.

By embedding verification habits into everyday workflows, organisations create behavioural barriers that attackers must overcome. Even highly convincing phishing emails or AI-generated messages become far less effective when employees consistently verify unexpected requests before acting.

In this way, verification discipline directly disrupts many of the social engineering techniques used by cybercriminals.

Secure Operational Behaviour

The third domain focuses on integrating secure behaviour into daily working practices.

Cybersecurity policies often describe the correct way to handle data, manage passwords, or use organisational systems. However, employees may bypass these procedures when they appear to slow down work or conflict with operational priorities.

Secure Operational Behaviour focuses on embedding security practices into normal workflows so that they become routine rather than exceptional.

For example, employees may be encouraged to adopt secure habits such as locking devices when leaving desks, using password managers instead of reusing credentials, and storing sensitive information within approved systems rather than external platforms.

These behaviours may appear simple, but they play a significant role in reducing the attack surface available to cybercriminals.

More importantly, when secure operational practices become normalised within an organisation, employees are more likely to notice deviations from expected behaviour. An unusual request for credentials, an attempt to bypass established processes, or a request to move information outside approved systems becomes more immediately suspicious.

By embedding secure practices into everyday operations, organisations reduce opportunities for attackers to exploit inconsistent behaviour.

Incident Judgement & Escalation

Even in well-secured environments, employees will occasionally encounter situations that appear suspicious but unclear. In these moments, the ability to exercise judgement and escalate concerns appropriately becomes critical.

Incident Judgement & Escalation focuses on ensuring that employees understand how to recognise potential incidents and feel confident reporting them.

Traditional training often encourages employees to report suspicious emails or unusual activity, but many staff hesitate to escalate concerns because they fear being wrong or wasting the security team's time.

Behaviour-led training addresses this barrier by emphasising that early reporting is a valuable security behaviour rather than an inconvenience.

For example, if an employee receives a suspicious email requesting login credentials, the correct response may not be to analyse the message extensively, but simply to report it to the organisation's security team. Early reporting allows security teams to identify broader attack campaigns and protect other employees. When escalation behaviour becomes normalised across the workforce, organisations gain a much earlier warning of potential threats.

Professional Cyber Judgement

The final domain focuses on organisational culture and professional responsibility. Cybersecurity is often viewed as the responsibility of IT departments or security specialists. However, modern organisations depend on employees across all roles interacting with digital systems, data, and communications. As a result, cybersecurity increasingly forms part of everyday professional responsibility.

Professional Cyber Judgement encourages employees to view cybersecurity

decisions as part of their role rather than as external rules imposed by security teams.

In practice, this means fostering a culture where individuals feel responsible for questioning unusual requests, protecting sensitive information, and supporting organisational security processes.

For example, an employee who receives an unusual request from a colleague may feel comfortable asking clarifying questions rather than assuming the request must be legitimate. Similarly, staff may proactively report suspicious communications rather than ignoring them.

When cybersecurity becomes embedded within professional identity, employees begin to see themselves as active participants in organisational defence.

Building Behavioural Cyber Resilience

Individually, each of the five domains addresses a specific aspect of cybersecurity behaviour. Together, they form a comprehensive behavioural framework that strengthens how employees recognise, evaluate, and respond to potential cyber threats.

By developing contextual awareness, verification discipline, secure operational practices, escalation confidence, and professional responsibility, organisations can transform their workforce into a powerful defensive layer within their cybersecurity strategy.

The Five-Domain Model therefore provides a practical structure for moving beyond awareness-based training and toward behavioural cybersecurity capability.

7. What Behaviour-Led Training Looks Like in Practice

If traditional cybersecurity awareness training focuses primarily on increasing knowledge, behaviour-led cybersecurity training focuses on changing how employees think and act when faced with potential cyber risk.

This difference fundamentally changes the way training is designed and delivered. Awareness-based training typically follows an information-delivery model. Employees are presented with examples of cyber threats, explanations of security policies, and lists of warning signs that may indicate malicious activity. Learning is often delivered through slides, short videos, or online modules, followed by multiple-choice quizzes that assess whether the participant can correctly identify the information that was presented.

Behaviour-led cybersecurity training takes a different approach. Rather than asking employees to memorise indicators of cyber threats, the training focuses on developing the judgement and behavioural habits required to respond securely in realistic situations.

Participants are placed in scenarios that mirror the types of decisions they encounter in their daily work. Instead of being told the correct answer in advance, they are asked to analyse situations, question assumptions, and determine how they would respond.

For example, a training exercise may present a realistic email from what appears to be a senior colleague requesting urgent action. The message may contain no obvious indicators of fraud. Participants are asked to decide whether they would act on the request, what questions they would ask, and how they would verify the instruction.

Through guided discussion, participants explore the reasoning behind their decisions and identify the behavioural cues that indicate potential risk.

This approach serves two important purposes. First, it exposes employees to the types of ambiguous situations that attackers commonly create. Second, it encourages individuals to develop the habit of pausing, evaluating context, and applying verification practices before acting.

A key behavioural principle used within behaviour-led training is “Pause and Verify.” Many successful cyber attacks rely on triggering an immediate response from the recipient. Messages are deliberately designed to create urgency, appear to come from authority figures, or resemble routine operational requests in order to encourage employees to act quickly. When individuals respond automatically to these pressures, they may bypass the checks that would normally prevent compromise.

The “Pause and Verify” principle introduces a deliberate interruption to this automatic response. Employees are encouraged to pause when encountering unexpected or unusual requests, particularly when the request involves sensitive information, financial transactions, or urgent action. This pause creates the opportunity to evaluate the context of the request and apply verification practices before responding.

Verification may involve confirming instructions through an alternative communication channel, checking the request against established organisational procedures, or seeking clarification from a colleague or manager. By embedding the habit of pausing and verifying before acting, organisations introduce a behavioural safeguard that can disrupt many forms of social engineering attack.
Behaviour-led training therefore shifts the emphasis from recognising obvious threats to managing uncertainty.

Another key feature of behaviour-led training is the emphasis on decision-making under realistic operational pressure. Employees rarely encounter cyber threats in isolation. Suspicious emails arrive alongside legitimate communications. Fraudulent requests often mimic normal business processes. Attackers deliberately design messages that blend seamlessly into everyday workflows.

Training exercises therefore reflect these conditions. Participants may analyse communication chains, evaluate conflicting information, or discuss how

compliance controls, ensuring that policies are documented, regulatory obligations are met, and employees receive the necessary guidance required by organisational standards and external frameworks.

However, the effectiveness of both technical and compliance controls ultimately depends on how employees behave when interacting with systems, communications, and data.

This introduces a third and often overlooked layer of defence: behavioural controls. Behavioural controls exist in the everyday decisions employees make when responding to emails, approving requests, handling information, or interacting with digital systems. These decisions determine whether security procedures are followed, whether suspicious activity is recognised, and whether potential incidents are escalated.

In practical terms, cybersecurity can therefore be understood as a shared organisational capability:

- IT manages the technical controls that protect infrastructure
- HR and governance functions oversee compliance and policy controls
- the wider workforce provides behavioural controls through everyday decision-making

When this behavioural layer is weak, even well-designed technical systems can be bypassed. Conversely, when employees develop strong verification habits, risk recognition skills, and escalation confidence, they become an active defensive capability rather than a passive vulnerability.

This means cybersecurity must be treated as an organisational capability rather than a specialist technical function. Every employee who interacts with digital systems plays a role in protecting the organisation.

Training programmes, therefore, must be designed not only for IT professionals but for the wider workforce whose everyday decisions influence cybersecurity outcomes.

Moving Beyond Compliance-Based Training

Another implication concerns how organisations approach cybersecurity education.

Many awareness programmes are delivered primarily to satisfy regulatory or compliance requirements. Employees complete training modules, pass knowledge-based assessments, and acknowledge organisational policies.

While these activities demonstrate that training has been delivered, they do not necessarily ensure that employees are capable of responding securely in real-world situations.

If the objective is to reduce cyber risk, training must focus on developing behavioural capabilities such as recognising unusual requests, verifying instructions, questioning unexpected activity, and escalating potential incidents. This requires training that reflects real operational conditions rather than simply delivering theoretical knowledge.

Measuring Behaviour Rather Than Training Completion

Organisations must also reconsider how they measure the effectiveness of cybersecurity initiatives.

Completion rates and assessment scores provide limited insight into how employees behave when confronted with real threats. An employee may correctly identify phishing indicators during a training quiz but still respond to a convincing social engineering message during a busy workday.

More meaningful indicators of security capability include behavioural metrics such as how frequently suspicious communications are reported, how consistently verification procedures are followed, and how quickly potential incidents are escalated.

These indicators provide a clearer picture of how the workforce contributes to organisational security.

Embedding Security Into Everyday Work

For behaviour-led cybersecurity to succeed, secure behaviour must be embedded within everyday operational processes.

Employees are more likely to follow security practices when those practices align with how work is actually performed. Clear verification procedures, accessible escalation channels, and practical guidance on handling unusual requests help employees respond appropriately without disrupting productivity.

When security behaviours are integrated into normal workflows, they become part of routine professional practice rather than additional tasks imposed by technical teams.

The Workforce as a Security Control

Finally, organisations should recognise that employees are not simply potential sources of cyber risk. When properly trained, they represent one of the most powerful security controls available.

Employees are often the first individuals to encounter phishing emails, fraudulent requests, or suspicious communications. If they possess the behavioural capability to recognise and question these interactions, attacks can be interrupted long before technical monitoring systems detect malicious activity.

Developing this capability transforms the workforce from a potential vulnerability into an active defensive layer within the organisation's cybersecurity strategy.

As cyber threats continue to evolve and attackers increasingly exploit human behaviour, organisations that strengthen this behavioural layer will be far better positioned to detect and disrupt attacks.

Conclusion

For more than a decade, cybersecurity awareness training has been widely promoted as a solution to the human element of cyber risk. Organisations have invested significant time and resources into training programmes designed to educate employees about phishing, password security, and safe online behaviour.

These efforts have played an important role in raising awareness of cybersecurity across the workforce. Employees today are generally far more familiar with common cyber threats than they were in the early days of corporate security training.

However, the persistence of human-enabled breaches demonstrates that awareness alone is not enough.

Employees frequently encounter cyber threats not in controlled training environments but within complex, fast-paced working conditions. They are expected to make rapid decisions while balancing operational priorities, responding to urgent requests, and navigating ambiguous information. Attackers deliberately exploit these pressures, designing social engineering campaigns that mimic legitimate communications and blend seamlessly into normal business activity.

Under these circumstances, cybersecurity failures are rarely the result of employees lacking knowledge about cyber threats. More often, they occur because individuals are placed in situations where behavioural judgement, verification discipline, and escalation confidence determine the outcome.

This distinction is critical.

If organisations continue to treat cybersecurity training primarily as a knowledge-transfer exercise, they risk addressing the symptoms of cyber risk rather than the underlying behavioural drivers.

Reducing human-related cyber risk requires a different approach — one that recognises cybersecurity as a behavioural capability embedded within everyday organisational activity.

Behaviour-led cybersecurity training represents this next stage of maturity.

Rather than focusing solely on teaching employees what cyber threats look like, behaviour-led training develops the practical decision-making skills required to

manage cyber risk in real-world environments. It emphasises contextual awareness, verification habits, operational discipline, and the confidence to escalate concerns when something appears unusual.

The Cyber Rebels Five-Domain Model provides a structured framework for developing these behavioural capabilities across the workforce. By strengthening contextual risk recognition, verification practices, secure operational behaviour, incident judgement, and professional cyber responsibility, organisations can transform employees from potential points of failure into active participants in organisational defence.

As cyber threats continue to evolve — and as technologies such as artificial intelligence enable attackers to generate increasingly convincing communications, impersonations, and digital deception — the ability of employees to exercise sound judgement will become even more important.

Technical controls will remain essential, and compliance frameworks will continue to guide organisational policy. But the effectiveness of these measures will ultimately depend on how people behave when confronted with uncertainty, urgency, and manipulation.

The future of cybersecurity training therefore lies not in increasing awareness alone, but in developing the behavioural capabilities that allow individuals and organisations to respond securely in the face of evolving threats.

Organisations that recognise and invest in this behavioural dimension of cybersecurity will be significantly better positioned to detect, disrupt, and withstand modern cyber attacks.

References

Verizon. (2024). Data Breach Investigations Report. Verizon Enterprise.
This annual report analyses thousands of real-world security incidents and consistently highlights the role of human behaviour in cyber breaches, including phishing, credential theft, and social engineering.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework). NIST.
The NIST Cybersecurity Framework provides guidance for organisations on managing cybersecurity risk and emphasises the importance of security awareness and workforce training.

ISO/IEC. (2022). ISO/IEC 27001: Information Security Management Systems – Requirements. International Organization for Standardization.
ISO 27001 establishes global standards for information security management and requires organisations to ensure personnel are aware of their information security responsibilities.

UK National Cyber Security Centre. (2023). Cyber Essentials Scheme. National Cyber Security Centre (NCSC).
The Cyber Essentials framework provides baseline cybersecurity controls for organisations and highlights the role of user awareness and secure behaviour in reducing cyber risk.

Verizon. (2023). Human Element in Cybersecurity – Data Breach Investigations Insights. Verizon Enterprise.
Analysis within the DBIR shows that the human element continues to play a role in the majority of security breaches, often through social engineering or credential misuse.

National Cyber Security Centre. (2023). Phishing Attacks: Defending Your Organisation. NCSC Guidance.
This guidance explains how attackers exploit human behaviour and organisational processes to deliver successful phishing campaigns.

About the Author

Andy Longhurst is the Founder of Cyber Rebels, a cybersecurity training company specialising in behaviour-led cybersecurity training for organisations.

With a background spanning technology, education, and business, Andy focuses on helping organisations develop the practical decision-making capabilities employees need to manage cyber risk in real-world environments. His work centres on the idea that cybersecurity failures are often behavioural rather than purely technical, and that effective training must therefore reflect how people actually work and make decisions.

Andy developed the Cyber Rebels Five-Domain Model, a framework designed to strengthen organisational cybersecurity capability by focusing on behavioural skills such as contextual risk recognition, verification discipline, secure operational behaviour, incident judgement, and professional cyber responsibility.

Through Cyber Rebels, he delivers practical, scenario-driven training designed to help organisations move beyond traditional awareness programmes and build stronger behavioural resilience against modern cyber threats.

More information about Andy and his work can be found at:
https://cyber-rebels.co.uk