MetaCompliance®

Cyber Security Awareness:

A Leader's Guide to Reducing Human Risk

Empowering teams to be your strongest line of defence against cyber threats.

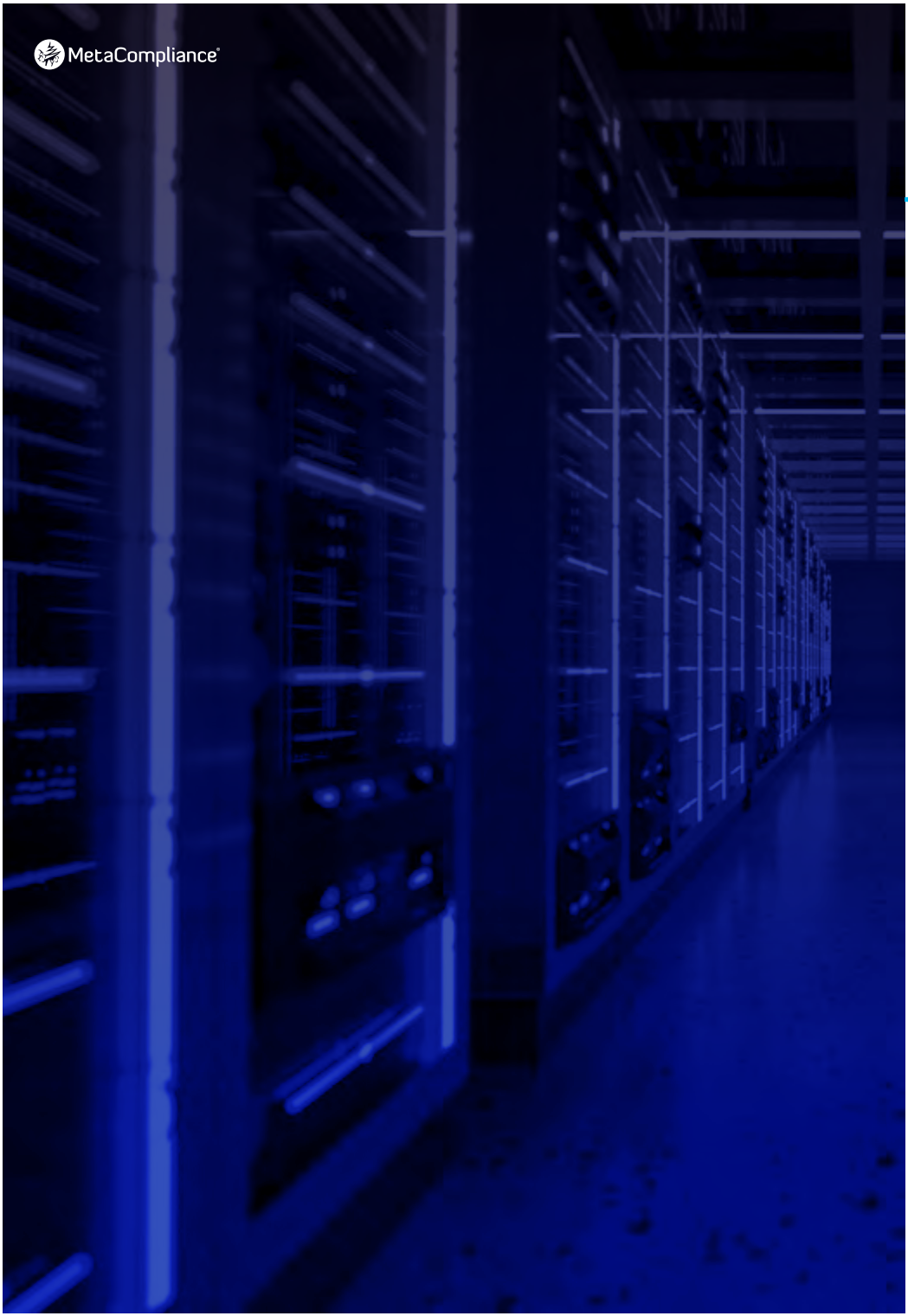
This guide gives leaders and managers the knowledge, strategies, and tools to build a security-first culture that protects their organisation.

MetaCompliance

Contents

MetaCompliance

Contents


MetaCompliance

Introduction

Technology is moving fast, and so are the expectations on leadership to manage cyber risk with understanding and control.

In 2026, cyber security is under sustained scrutiny. Boards expect evidence, regulators expect proof, and customers expect reassurance. Having controls in place just isn't enough. Organisations are expected to demonstrate that those controls are reducing cyber risk in practice.

Attackers continue to rely on familiar tactics, with urgency, authority, social engineering, and exploiting distraction and fatigue all taking centre stage. Even the strongest technical environments remain exposed when cyber risk at the human layer is left unmanaged.

That's why cyber resilience should be treated as a core business priority. It requires leadership ownership, measurable outcomes, and a culture that understands its role in reducing cyber risk.

The impact of a cyber incident now extends far beyond financial loss; regulatory exposure, executive accountability, operational disruption and reputational damage are also at stake. Cyber risk is a business risk, and it demands the same discipline as financial and operational oversight.

This guide provides practical direction for leaders who want to strengthen security awareness and human risk management, build lasting behavioural change, and demonstrate measurable reduction in cyber risk across their organisation.

If your organisation has invested in technology and now needs to evidence real-world resilience, this is where to begin.

Who This Guide is For

This guide is designed for:

- **Senior leaders and executives** who set strategy and need to understand the risks and responsibilities of cyber security at board level.
- **HR, compliance, and L&D teams** responsible for education, culture, and regulatory adherence.
- **IT and security managers** who want to align technical controls with employee behaviour.
- **Line managers and team leaders** who influence day-to-day staff engagement and compliance.

If you're involved in protecting sensitive business data, managing human risk, or shaping cyber security culture, this guide is for you.

How to Use This Guide

We've designed this guide to be practical and easy to apply. You don't need to read it cover to cover (though you can). Instead:

- **Scan for quick wins:** Each chapter includes tips you can act on immediately.
- **Apply the actions:** Use the examples, checklists, and recommendations to shape your awareness campaigns and policies.
- **Think long-term:** The frameworks and practical strategies are there to help you build resilience, not just tick compliance boxes.
- **Measure progress:** Look out for the sections that highlight how to track engagement and success.

Keep this guide close at hand. Reference it when planning cyber awareness campaigns, updating policies, or making the case for investment in human risk management and security awareness.


MetaCompliance

Chapter 1

Understanding the Modern Cyber Security Landscape

Surveying the evolving threat landscape

Cybercrime has become one of the most persistent and damaging risks to modern organisations. In 2025 alone, global cybercrime costs were estimated in the trillions of dollars[1], placing it among the most significant economic threats worldwide. Attackers are well-funded, highly organised, and constantly adapting their tactics.

Today, cyber threats rarely rely on brute-force hacking alone; they exploit people, processes, and supply chains as much as technology. Social engineering, AI-generated content, and impersonation techniques now sit alongside traditional malware and network attacks. In many reported incidents, human error remains a contributing factor in over 70% of breaches[2], reinforcing the importance of addressing behaviour as well as systems.

To reduce cyber risk, organisations must understand the different threats targeting their people and systems, and how those threats continue to evolve.

Common cyber threats that target people

Phishing

Still the most common entry point for attacks, phishing uses email, text, collaboration tools, or social media messages to trick recipients into sharing credentials, downloading malicious files, or visiting fake websites. The 2025 Verizon Data Breach Investigations Report (DBIR)[3] highlights that phishing remains a dominant threat vector, accounting for 19% of breaches and frequently serving as the initial entry point in complex, human-centric attacks, which contribute to roughly 60% of all breaches. Key findings include a surge in AI-generated phishing, a 30% jump in third-party involvement, and the critical role of recent, consistent security training in improving employee reporting rates.

AI has significantly increased the effectiveness of these attacks. Messages can now be generated at scale, tailored to specific roles or individuals, and reinforced through follow-up contact across multiple channels, including collaboration platforms and voice communication. Increasingly, phishing campaigns are supported by deepfake audio or video, allowing attackers to convincingly impersonate senior leaders, suppliers, or colleagues. Once trust is established, attackers can harvest login details, install malware, or launch wider business email compromise (BEC) campaigns.

In addition to direct phishing messages, attackers increasingly use so-called “watering hole” tactics. Rather than contacting victims directly, they compromise websites that a specific group frequently visits, such as industry forums, supplier portals, or professional communities. When users visit these trusted sites as part of their normal workflow, malicious code can silently harvest credentials or deliver malware. Because the interaction appears routine and familiar, suspicion is significantly reduced.

Malware

Malware, short for malicious software, includes viruses, worms, trojans, spyware, and ransomware. It can be installed when users click a link, download a file, or connect an infected device. Ransomware in particular continues to rise, with average ransom demands now reaching millions of dollars[4] per incident, and recovery costs often far exceeding the ransom itself.

Once active, malware may steal, encrypt, or delete data, disrupt key systems, or demand ransom payments. Increasingly, malware is used to establish long-term access to corporate networks for further exploitation, rather than causing immediate disruption.

A growing variation of social engineering involves persuading users to execute malicious commands themselves. In so-called "ClickFix" style attacks, victims are shown fake error messages or technical prompts instructing them to press specific key combinations or copy and paste commands into their system to "resolve" an issue. By convincing users to initiate the action voluntarily, attackers can bypass certain automated security controls and establish access without exploiting a traditional software vulnerability.

AI-driven impersonation and deepfakes

Advances in artificial intelligence have introduced a new class of human-focused cyber threats: AI-driven impersonation and deepfakes. These attacks use generative AI to convincingly mimic the voice, appearance, writing style, or behaviour of real people, including senior leaders, colleagues, suppliers, or public figures.

Deepfake audio and video can now be produced quickly and cheaply, making it possible for attackers to create realistic phone calls, voice notes, video messages, or live video calls that appear legitimate. When combined with information gathered from social media or previous breaches, these attacks can be highly targeted and difficult to distinguish from genuine communication.

These techniques are increasingly used to support phishing and business email compromise (BEC) attacks, adding pressure and credibility to urgent payment requests, credential resets, or changes to banking details. Because they exploit trust and familiarity rather than technical vulnerabilities, traditional security controls on their own may not detect them.

Attacks targeting human use of AI systems

As organisations integrate AI tools into daily operations, attackers are beginning to target the human-AI interaction layer itself. One emerging technique, known as prompt injection, involves embedding hidden or misleading instructions within content that an AI system processes.

These instructions may attempt to override safeguards, extract sensitive data, or manipulate outputs in ways that appear legitimate.

When humans rely on AI-generated responses without understanding how those outputs may have been influenced, the risk increases. Attackers may deliberately craft documents, emails, or web content designed to influence both the AI system and the human reviewing its output. As AI adoption grows across customer support, coding, analysis, and research workflows, organisations must consider not only technical AI security controls but also the human judgement surrounding AI-generated information.

Business Email Compromise (BEC)

BEC attacks focus on manipulating trust rather than deploying malware. Attackers impersonate executives, finance teams, or trusted suppliers to request urgent payments or sensitive information. These attacks are often highly targeted and difficult to detect, and globally account for trillions in reported losses[5] each year.

AI-generated emails, voice cloning, and deepfake video calls have made BEC even more convincing, increasing the pressure on employees to act quickly without verification. These attacks increasingly extend beyond email, combining written requests with voice notes, video calls, or messages on collaboration platforms to reinforce legitimacy and increase pressure to act quickly.

Insider threats

Not all threats come from the outside. Insider risks arise when employees, contractors, or third-party partners misuse their access, intentionally or by mistake. This could be a disgruntled former employee stealing data, or a well-meaning colleague falling for a phishing email or mishandling sensitive information.

With hybrid working, cloud platforms, and shared collaboration tools now standard operating models, managing access and monitoring insider risk has become a continuous challenge rather than a one-time project.

Supply chain attacks

Modern organisations rely on vast networks of suppliers and service providers and cybercriminals increasingly look for opportunities within the wider supply chain. Interconnected systems and shared data can provide alternative routes into larger organisations.

Recent high-profile breaches have shown that a single compromised vendor can impact hundreds or thousands of downstream organisations, making third-party risk management and shared awareness now a business-critical issue.

Why human behaviour remains the biggest variable

Technology continues to advance, but human behaviour remains broadly consistent. Attackers exploit curiosity, trust, fear, and urgency; the same emotional triggers that influence everyday decisions at work.

This is why focusing solely on security awareness education, while still essential, is no longer sufficient.

Organisations are increasingly shifting toward Human Risk Management (HRM), an evolution of traditional security awareness training that centres on understanding, measuring, and reducing risky behaviour over time.

HRM extends beyond one-off learning modules. It incorporates behavioural analytics, threat intelligence, and system integrations to identify patterns of risky activity and intervene early. By combining real-world threat data with user behaviour insights, organisations can better anticipate where human-related cyber risk may emerge and take proactive steps to reduce exposure.

Building a cyber-aware culture requires empowering individuals to recognise, report, and respond to threats with confidence. When employees understand how attacks work, feel supported in raising concerns, and operate within systems designed to reinforce safe behaviours, they become an active and measurable component of the organisation's defence strategy.

Making security awareness part of digital transformation

Digital change is now continuous. Cloud platforms, automation, AI-enabled tools, and flexible working models are embedded into day-to-day operations and each change expands both opportunity and risk.

Embedding cyber awareness and human risk management early ensures that security isn't an afterthought, but a foundation of sustainable growth.

Practical steps include:

- Integrating awareness education and HRM principles, such as measuring, influencing, and reducing risky behaviours, into system upgrades, process changes, and tool adoption
- Running simulated phishing and impersonation exercises alongside platform changes or organisational restructures
- Embedding updated policies and regulatory expectations into change communications, so security expectations are clear from day one
- Encouraging collaboration between IT, HR, compliance and business leaders to keep messaging consistent
- Promoting clear reporting channels so employees know how, and when, to raise concerns
- Establishing reporting dashboards and measurable risk metrics, so behavioural data becomes a shared source of truth and a benchmark for continuous improvement

Reporting suspected incidents should be positioned as a positive behaviour. High reporting rates allow organisations to measure human risk, identify trends, and demonstrate improvement over time, turning awareness programmes into data-driven boardroom conversations.

Navigating frameworks and regulation

Cyber security awareness and human risk management don't sit in isolation. They underpin recognised frameworks such as ISO/IEC 27001:2022[6] and the NIST Cyber Security Framework 2.0[7], both of which emphasise governance, resilience, and the critical role people play in preventing, detecting, and responding to threats.

Regulation is reinforcing this shift. Standards like the EU General Data Protection Regulation[8] (GDPR) and the Digital Operational Resilience Act[9] (DORA) make it clear that organisations must demonstrate operational readiness, tested response plans, and employee awareness; not just technical safeguards. While DORA applies specifically to financial entities and their ICT providers, its principles of clear accountability, third-party oversight, and resilience testing are increasingly shaping expectations across other sectors.

Emerging regulation is also beginning to address the risks introduced by artificial intelligence. The EU Artificial Intelligence Act[10] (AI Act) introduces a risk-based framework for the development and use of AI systems, with specific expectations around transparency, accountability, and human oversight. While the AI Act is not a cyber security regulation, it reinforces the importance of understanding how AI-enabled systems influence behaviour, decision-making, and trust.

As AI becomes more embedded in business processes, communication tools, and security operations, organisations will increasingly need to demonstrate that employees understand how AI is used, where its limitations lie, and when human judgement and verification are required. This further strengthens the role of awareness, governance, and measurable human risk management in maintaining resilience.

In 2026, organisations are facing a more complex and fast-evolving regulatory environment. New and updated legislation — such as the EU's NIS2 Directive[11] and Cyber Resilience Act[12], the UK's Cyber Security and Resilience Bill[13], and updated regulatory guidance from bodies like SEC and APRA — continues to raise expectations around governance, supply chain risk, operational resilience, and the human role in security. This makes it more important than ever to understand not just what regulations exist, but which ones genuinely apply to your organisation.

Rather than attempting to track every regulation individually, a more sustainable approach is to focus on applicability and alignment.

To do this effectively, organisations should:

Map regulatory exposure by geography, sector, and the types of data and services they provide, including where data is processed or accessed by third parties

Assign clear ownership for monitoring regulatory change, ensuring responsibility sits with named roles rather than being shared vaguely across teams

Use recognised frameworks such as ISO 27001 and NIST CSF as a baseline, then map regulatory requirements to existing controls and behaviours

Align awareness and Human Risk Management metrics with audit, risk, and compliance reporting, so evidence of effectiveness is readily available

Focus on proof, not presence, using reporting data, simulations, and behavioural trends to demonstrate how people are supporting resilience in practice

By anchoring regulatory compliance to trusted frameworks and measurable human behaviour, organisations avoid reactive, checkbox-driven compliance responses. Instead, they build a defensible, adaptable security posture that can respond to regulatory change without constant reinvention.

Understanding attacker profiles and motivations

Not all cybercriminals look alike or act for the same reasons. Forget the Hollywood stereotype of the hooded figure in a dark room. Today's attackers range from organised criminal groups to lone insiders, from hacktivists to state-sponsored actors. Understanding what motivates them helps organisations anticipate the kinds of threats they may face and prepare a more targeted defence.

Financial gain

Money remains the number one driver of cybercrime. Ransomware gangs, business email compromise (BEC) operations, and online fraud schemes all rely on exploiting human behaviour to turn a profit.

While large-scale attacks make headlines, smaller businesses are increasingly targeted because they're often less protected and easier to monetise. A coordinated campaign against ten small firms can yield the same financial reward as one high-profile breach, with far less effort and attention.

Espionage and nation-state activity

Cyber espionage — stealing sensitive data, intellectual property, or trade secrets — is no longer limited to governments. Private companies, research institutions, and critical infrastructure providers have all become targets.

State-sponsored attackers may aim to disrupt services, gain strategic advantage, or undermine trust in institutions. These operations are often sophisticated and long-term, using social engineering and targeted phishing to exploit the human layer of defence before moving deeper into networks.

That's why mobilising your workforce as part of your defence strategy is so important. Technical measures can't detect every deceptive email or unusual request, but people can.

Challenge and recognition

Some attackers are driven by curiosity, competition, or reputation. "White-hat" and "grey-hat" hackers often operate in this space, testing

systems for flaws, sometimes with good intentions, and sometimes for bragging rights or prizes. Ethical hacking competitions like Pwn2Own have shown how quickly skilled professionals can uncover vulnerabilities that even major brands overlook.

While this kind of activity can benefit security research, it also highlights how accessible hacking tools and knowledge have become.

Hacktivism

Hacktivists use cyberattacks to promote a political or social cause; from disrupting websites to leaking confidential data. Because these campaigns are often public and symbolic, they can damage reputation as much as infrastructure.

Advances in automation and social media amplification have made hacktivism cheaper, faster, and more visible than ever before, allowing small groups to have outsized impact.

Resource theft

Not every attack focuses on stealing data. Some criminals hijack computing power to mine cryptocurrency; a tactic known as cryptojacking. Infected websites, compromised Wi-Fi networks, or malicious browser extensions can quietly drain resources from users and organisations without their knowledge.

The growing profitability of digital assets has made this a persistent low-level threat, particularly for organisations managing large device fleets or cloud environments.

Human error and insider risk

Beyond deliberate attacks, many incidents stem from within; whether it's a misconfigured cloud storage bucket, an unpatched application, or an employee sharing sensitive information unintentionally. These are often the hardest risks to predict because they arise from everyday actions.

Regular security awareness training, robust access controls, and a supportive reporting culture are essential to reduce the likelihood and impact of these errors.

Security frameworks and data protection

Strong cyber security is about having the right frameworks, processes, and people in place to keep information safe and systems resilient.

Before you start mapping out a security programme, it's worth asking two key questions:

- How can we build a security management system or framework that's right for our organisation?
- What are the moving parts that need to work together to make it effective?

Several well-established frameworks can help you answer those questions.

ISO/IEC 27001:2022 — the global standard for information security

ISO 27001 remains the gold standard for information security management systems (ISMS). It provides a clear, structured approach to identifying risks, protecting data, and continually improving controls.

Unlike many frameworks, ISO 27001 is externally audited and certifiable, meaning your organisation can formally demonstrate its commitment to information security and governance. For many customers and partners, that certification is now a minimum expectation, especially within supply chains.

Achieving and maintaining ISO 27001 requires leadership involvement and ongoing awareness across the business. It's not a one-off project; it's a culture shift.

The benefits of ISO 27001 include:

- Greater business resilience and protection against incidents
- Stronger customer and stakeholder confidence
- More consistent processes for managing and reviewing risk
- Clear accountability across departments

Why staff awareness matters for ISO 27001 compliance

ISO 27001:2022 places significant emphasis on competence and awareness, particularly in clauses 7.2 to 7.4, which require employees to understand their roles within the Information Security Management Systems (ISMS).

Generic cyber security education isn't enough. Awareness needs to be tailored to your organisation's specific risks, policies, and controls. That might mean:

- Running short briefings or webinars explaining how your ISMS works
- Aligning awareness campaigns with policy updates or audit cycles
- Reinforcing key concepts like incident reporting, data classification, and physical security

By grounding your awareness programme in your own ISMS, you avoid fatigue and ensure every message is relevant and actionable. As threats evolve, your ISMS — and the education that supports it — should evolve too.

The NIST Cyber Security Framework 2.0

Developed by the U.S. National Institute of Standards and Technology, the NIST Cyber Security Framework[14] (CSF) provides a voluntary, risk-based framework for managing and reducing cyber security risk. Originally designed for critical infrastructure, it's now widely adopted across industries and geographies as a common reference point for structuring cyber security programmes.

The framework offers a flexible structure that organisations can adapt to their size, sector, and risk profile. It covers governance, risk management, technical safeguards, detection, response, and recovery activities, creating a shared language between technical teams, executives, and regulators.

The updated CSF 2.0, released in 2024, reflects today's interconnected digital risks and formally introduces a new core function: Govern. This addition reinforces the importance of leadership oversight, accountability, supply chain risk management, and alignment between cyber security strategy and broader business objectives.

The framework is built around six core functions:

1. **Govern**
   Establish leadership, accountability, and oversight for managing cyber risk.
2. **Identify**
   Understand assets, data, and risks.
3. **Protect**
   Implement safeguards to limit impact.
4. **Detect**
   Identify potential incidents quickly.
5. **Respond**
   Contain and mitigate threats effectively.
6. **Recover**
   Restore systems and strengthen resilience for the future.

Together, these functions form a cycle of continuous improvement — helping organisations measure maturity, prioritise investment, and build shared understanding between technical and non-technical teams.

Regulation and operational resilience

Across jurisdictions, regulation is catching up with reality. Regulation like the EU General Data Protection Regulation (GDPR), the UK Data Protection Act 2018, and the EU Digital Operational Resilience Act (DORA) all reinforce the expectation that organisations must not only secure data but prove they can recover from disruption.

DORA, in particular, highlights the growing link between governance, cyber awareness, and operational continuity. It applies to financial institutions and the ICT providers that support them, but its principles, clear accountability, tested response plans, and a culture of readiness, apply to any organisation managing digital services.

The importance of staff awareness in digital transformation projects

Digital transformation offers enormous opportunity: new technologies, smarter processes, and better customer experiences. But transformation also brings change, and with change comes risk.

When organisations adopt new platforms or automate key functions, the focus often falls on innovation and efficiency. Security and compliance can easily become an afterthought. Yet every new system, integration, or workflow creates potential entry points for attackers and new responsibilities for employees.

Transformation projects aren't just about technology; they're large-scale change management programmes that depend on people. Success relies on communication, clarity, and shared accountability.

That means security awareness should be embedded into transformation plans from the very start. Teams need to understand not only how to use new systems, but how to do so safely, recognising risks such as data leakage, phishing during system migrations, or misconfigured cloud environments.

Practical steps include:

- Involving security teams early in project planning
- Running short awareness sessions alongside rollouts and upgrades
- Building security messaging into digital change communications
- Encouraging employees to question unusual requests or behaviours during transitions

Striking the right balance between innovation and security isn't about slowing progress — it's about making transformation sustainable. When staff feel informed, supported, and confident, they become active partners in protecting the organisation as it evolves.

Key takeaway

Cyber threats are no longer just a technical issue, they're a measurable human risk. Modern attacks exploit trust, speed, and behaviour as much as vulnerabilities in systems.

A strong defence starts with understanding how threats evolve, embedding security awareness learning into everyday operations, and evolving toward Human Risk Management; where behaviour is observed, reported, measured, and improved over time.

Organisations that combine trusted frameworks like ISO 27001 and NIST CSF 2.0 with continuous awareness and meaningful reporting move beyond education alone. They gain visibility into human risk, can track behavioural trends over time, and use that insight to inform decisions, strengthen controls, and involve employees as an active part of their defence.


MetaCompliance
2

Chapter 2

Cyber Resilience in the Age of AI

When innovation becomes exploitation

Artificial Intelligence (AI) has transformed how we live and work; automating repetitive tasks, improving efficiency, and powering faster, smarter decisions. But the same tools driving progress are now being weaponised by cybercriminals, creating a new generation of intelligent, scalable attacks that blend seamlessly into everyday business activity.

AI has lowered the barriers to entry for attackers. What once required advanced technical skill can now be achieved using widely available generative tools. Phishing emails, fake websites, deepfakes, synthetic voices and malicious chatbots can be produced in seconds; personalised, polished, and increasingly difficult to distinguish from legitimate communication.

By 2025[15], security teams reported that AI-assisted phishing and impersonation techniques had become a routine feature of real-world attacks, rather than an emerging trend. In many organisations, simulated phishing data shows higher click-through and response rates when AI-generated language is used, particularly in executive and finance-focused

scenarios — for example, Microsoft's Digital Defense Report 2025[16] found AI generated phishing emails achieving clickthrough rates around 54 % compared with roughly 12% for traditional messages, illustrating the increased effectiveness of more sophisticated, language in tricking users.

This isn't just a technical shift; it's a psychological one. AI can now convincingly mimic writing styles, voices, and even faces. In one widely reported case, a finance employee authorised a $25 million transfer after a deepfake video call featuring realistic, but fake versions of senior executives. Similar incidents have since been reported across multiple regions and sectors.

When technology can impersonate trust at scale, human judgement, supported by the right structures and data, becomes the ultimate line of defence.

The expanding human attack surface

AI has made attacks faster, cheaper, and more believable. But it's has also widened the human attack surface. Employees increasingly rely on AI tools to write emails, summarise data, analyse documents or brainstorm ideas; sometimes sharing sensitive or regulated information without realising the potential consequences.

When staff paste confidential text into public or poorly governed AI platforms, that data may be logged, retained or reused in ways the organisation cannot control. Combined with the growing sophistication of AI-powered scams, this creates a feedback loop: the more data employees share, the more realistic future attacks can become.

Agentic AI systems compound this cyber risk. Any system that automatically parses or acts on input, such as summarising an email, extracting data from a document or triggering a workflow, becomes part of the attack surface. A hidden prompt embedded in an email may be ignored by a human reader, yet interpreted and executed instantly by an AI agent. Prompt injection attacks exploit that gap, turning trusted automation into an unintended pathway for compromise.

Every interaction, whether an email, a chat message, a document upload or a voice call, can now create exposure. The frontline of cyber security has shifted. Protecting infrastructure remains critical, but organisations must also understand, measure and reduce cyber risk at the human layer.

From awareness to action: Human Risk Management and AI

Traditional security awareness training remains important, but on its own it can't keep pace with AI-driven threats. Attackers now iterate in real time, adapting tone, language, and tactics faster than static or annual learning programmes can respond.

Human Risk Management (HRM) represents the evolution of security awareness training. Rather than focusing solely on knowledge transfer, HRM concentrates on behavioural risk, using continuous learning, realistic simulations, reporting data, and measurable outcomes to improve decision-making over time.

Instead of simply telling people what not to do, HRM helps organisations identify where risky behaviours occur, understand why they happen, and support employees in making safer choices. This shift is critical in an environment where even well-informed staff can be convincingly deceived.

HRM builds resilience through:

- Continuous education and awareness, reinforced through ongoing microlearning rather than one-off training.
- Role-specific training and simulations that mirror real-world AI-enabled threats such as deepfake video calls, voice phishing and prompt injection attacks.
- Regular updates on emerging risks and attack techniques, ensuring employees understand the latest threats and how to respond confidently.
- Clear reporting mechanisms that encourage employees to flag suspicious activity quickly and without fear of blame.
- Structured feedback loops that enable organisations to track progress, identify high-risk groups, and demonstrate measurable reduction in cyber risk over time.

By embedding awareness into daily workflows and by measuring how people actually respond to threats, organisations can transform their largest attack surface into a managed and measurable line of defence.

Building cyber resilience in your organisation

AI-powered attacks thrive on speed, scale and social pressure. To stay ahead, organisations must create cultures that value slowing down, thinking critically, and checking authenticity.

Core principles include:

Verification first: Encourage staff to confirm high-risk or unusual requests via secondary channels (e.g. phone, Teams, or in-person).

Multi-layered protection: Pair MFA, policy management, and phishing simulations with continuous education, simulations and HRM analytics.

Personalised learning: Tailor content to specific roles, regions, risk exposure and past behaviour so it feels relevant and practical.

Empowered employees: Make it clear that questioning suspicious activity, even if it appears to come from leadership, is expected and supported

Cyber resilience isn't just about eliminating mistakes; it's about detecting risk early, responding quickly, and using data to continuously reduce exposure as threats evolve.

Key takeaway

AI-enabled attacks succeed by exploiting speed, authority, and uncertainty. Defending against them requires more than awareness; it requires visibility into how people actually behave under pressure, and who is at more risk.

Organisations that build long-term cyber resilience focus on measuring human risk, not just delivering training. They track how employees respond to realistic threats, encourage early reporting, and use that data to target individuals with the right education at the right time, reduce repeat risk, and inform leadership decisions.

A strong Human Risk Management approach combines continuous learning, realistic simulations, and clear reporting pathways to turn human judgement into a controlled, measurable defence capability.

In an environment where trust can be convincingly faked, resilience comes from how quickly people question, verify, and report; and how effectively people learn from that behaviour over time.


MetaCompliance
3

Chapter 3

Establishing the Need for Cyber Security Awareness

Why awareness matters

For years, cyber security investment has focused on technology: firewalls, antivirus software, intrusion detection systems and access controls. These defences are essential, but they don't protect against the most unpredictable factor in any organisation: people.

One click on a phishing email, one weak or reused password, or one misdirected document can bypass even the most advanced technical controls. By 2025, regulators, insurers, and boards were increasingly aligned on one point: human risk is now a material business risk, with direct financial, operational, and regulatory consequences.

True resilience depends on more than technical safeguards, it requires awareness, leadership, and a culture where secure behaviour is understood, expected, and reinforced.

Understanding your organisation's risk profile

Every organisation faces a different mix of threats. To manage them effectively, you need to understand both likelihood and impact; what could go wrong, how often it might happen, and what the consequences would be.

Common exposure points include:

- **Staff behaviours** — accidental errors, risky shortcuts, or susceptibility to social engineering
- **Supply chains** — vulnerabilities introduced through third-party access or shared systems
- **Legacy platforms** — outdated infrastructure that can't support modern security controls

Mapping these vulnerabilities and developing mitigation plans is the foundation of any effective cyber awareness strategy and human risk management programme.

Building a risk awareness campaign

Security awareness campaigns shouldn't be about ticking boxes or rushing through annual learnings.

Real behavioural change requires consistent communication, ongoing reinforcement, and visible leadership support.

For many organisations, this has led to the evolution of traditional awareness programmes into Human Risk Management (HRM). HRM builds on the foundations of security education, but goes further by focusing on understanding, measuring, and reducing risky behaviours over time, using data, behavioural insight, and threat intelligence to guide interventions.

People are naturally resistant to change, especially when it disrupts established habits. That's why awareness must be delivered as part of a sustained cultural shift, not a one-off exercise. When employees see that secure behaviour is noticed, measured, and supported — not punished — engagement improves.

Measuring staff understanding of risk

Before you can improve awareness, you need to know where you stand. Baseline measurement is essential, not just for programme design, but for demonstrating progress to leadership and regulators.

Simple diagnostics can help you gauge current understanding:

- **Run simulated phishing** exercises to identify how many employees fall for realistic attacks, and how many report them.
- **Review past incidents** over the last 12 months (look for recurring themes, repeated errors or slow reporting.)

These data points help quantify human risk and create a defensible starting position for improvement. Use these insights to explain why awareness matters. For example:

> "Over the past quarter, we've seen a steady increase in lost or unsecured devices being reported. As part of our ongoing security awareness programme, we're reinforcing device security through short, regular learning nudges and reminders to reduce this risk over time."

Making risks relatable and education more frequent helps staff connect their daily actions to real consequences. Over time, repeating this measure–educate–retest cycle allows organisations to show reduced risk exposure and improve employee judgement — a key board-level conversation.

Targeting learning where it matters most

Effective awareness is targeted awareness. Generic learning materials delivered uniformly across the organisation often lead to disengagement, low retention and limited risk reduction – with industry benchmarks showing that without structured training, around 33% of employees will click on simulated phishing links[17], yet with ongoing, high-quality awareness and simulation training that can be reduced by up to 86% within a year. People experience risk differently depending on their role, access, authority, and working patterns, and awareness needs to reflect that reality.

Effective human risk management programmes use incident data, phishing results, reporting trends, and behavioural signals to identify where risk is concentrated to prioritise education accordingly. This allows organisations to move from broad, generic campaigns to focused interventions that address real exposure.

Role and department-based targeting is essential. For example:

- **Finance teams** are consistently targeted for payment fraud, business email compromise (BEC), and AI-enabled impersonation attacks. Education should focus on verification behaviours, payment change procedures and recognising urgency-based pressure tactics.
- **Privileged technical users** require deeper education on secure configuration, access management, automation risks, and the downstream impact of misconfiguration — not just general phishing awareness.
- **Executives and senior leaders** are prime targets due to their authority, public visibility, and access to sensitive data. Awareness for this group should be concise, scenario-led, and focused on decision-making under pressure, including deepfake voice and video risks.

Targeting should also reflect how people work and learn. Not everyone absorbs information in the same way, and effective programmes account for this:

- Desk-based staff may engage well with short eLearning and simulations.
- Frontline or field-based workers may need mobile-first content, brief videos, or in-the-moment prompts.
- Time-poor leaders often respond best to short, high-impact scenarios rather than long-form training.

Your supply chain partners should also be included, as they're part of your extended risk surface and are frequently targeted as alternative entry points. Third-party education should be proportionate to access and risk, focusing on the behaviours that matter most rather than replicating internal programmes in full.

Additional factors to consider include tenure, geography and language:

- **New joiners** often adapt quickly to policies but may lack context around real-world threats or historical incidents, making early, practical reinforcement critical.
- **Long-serving employees** may need extra support to unlearn old habits that don't align with modern systems, cloud environments, or AI-enabled risks.
- **Multilingual teams** require awareness materials in the languages they use daily, especially when phishing or AI-driven scams exploit local language, tone, and cultural cues to build trust.

By tailoring awareness to role, risk, and learning style, and adjusting it over time based on measurable behaviour, organisations reduce fatigue, increase relevance, and achieve meaningful risk reduction. This targeted approach is a core principle of Human Risk Management and a key driver of sustainable culture change.

Prioritising security alongside other business risks

Many organisations still view security as a technical or compliance issue rather than a core business risk. Financial exposure is tracked in detail, while cyber risk can feel abstract or secondary. PwC reports[18] that while 66% of leaders see cyber security as a business risk, just 2% of organisations have embedded enterprise-wide cyber resilience, leaving cyber exposure less tangible than financial risk.

Changing that mindset requires consistent messaging and board-level support. Awareness campaigns should highlight that the cost of inaction; regulatory fines, operational disruption, reputational damage, and the financial impact of a data breach itself (the global average cost of a breach is currently ~$4.44 million[19]) — is far greater than the effort required to embed secure habits. Using reporting data (phishing resilience, incident trends, reporting rates) helps translate cyber risk into familiar business metrics.

Legacy systems often add to the challenge. Staff may dismiss risks with comments like, “That’s just how our system works.” Communicate clearly that while full replacement may take time, mitigation and user vigilance are essential in the meantime —, especially during periods of transition, automation, or AI adoption.

Making cyber security real for people

Let’s face it: cyber security isn’t everyone’s favourite topic. Most employees spend little time thinking about it unless it’s presented in a way that feels engaging, relevant and achievable.

Participation is a critical success metric. If only half your workforce completes regular awareness traininglearning, you can’t demonstrate compliance or culture change, and the least engaged employees may be the most at risk.

To drive engagement:

- Use high-quality eLearning with strong visuals and relatable scenarios (including AI-enabled threats).
- Offer content in multiple languages and allow users to select their preference.
- Deliver learning where people already work, integrating awareness content into collaboration platforms, email environments, and everyday workflows.
- Incorporate short, interactive formats: quizzes, videos, and microlearning modules.
- Track participation and reporting behaviour, following up with supportive reminders and coaching rather than punitive measures.

When awareness feels practical, personalised, and easy to access, participation – and reporting – rises dramatically and risk reduces.

Managing risk through relevance

Nearly every organisation is undergoing some form of digital transformation, such as expanding cloud services, increasing automation, integrating AI-enabled tools and modernising legacy platforms. These initiatives introduce new efficiencies, but also new human and operational risks.

Regulations such as the EU GDPR, the UK Data Protection Act 2018, and DORA (for financial institutions and ICT vendors) all emphasise security by design, privacy by design and demonstrable operational resilience. Embedding awareness and HRM principles into these initiatives helps organisations prove not just intent, but effectiveness.

Embedding cyber awareness within transformation efforts also:

- Elevates the profile of security at board level
- Positions security as an enabler, not a blocker
- Helps project teams identify and mitigate risks earlier

When leadership evaluates transformation projects, they already assess financial and operational risks. Security and data protection should be ranked alongside them, informed by real behavioural data, not treated as separate concerns.

Key takeaway

Cyber security awareness isn't a standalone campaign; it's a continuous, measurable effort to align people, process, and technology around a shared goal: protecting what matters most.

By understanding your risk profile, identifying higher-risk users or behavioural patterns, targeting high-impact behaviours, encouraging reporting, and integrating awareness into business change, organisations can reduce exposure in a structured and measurable way.

They build a Human Risk Management framework that allows leaders to track risk reduction over time, demonstrate impact and make informed decisions at board level.


MetaCompliance
4

Chapter 4

Changing Organisational Culture with Cyber Security Awareness Campaigns

Start with behaviour change (not just activities)

It's tempting to jump straight into learning and simulated phishing to tackle cyber risk. But if the goal isn't behaviour change, the campaign will stall. Treat security awareness like any other change management programme: cross-functional, planned, and sustained. The objective is to reduce human risk over time, not simply to deliver training.

Bring together a multidisciplinary team, such as project management, internal comms/marketing, HR, IT/security, and legal/compliance, to co-own objectives, messages, timelines, and measurement. This shared ownership also ensures behavioural data, incident trends, and reporting insights are fed back into the programme.

Expect friction. Change takes time and energy, and other corporate initiatives will compete for attention. The answer isn't to stop; it's to pace communications so people can keep up.

Communicating like you mean it

Your campaign should feel like it belongs to your organisation.

Brand it: Use your visual identity so it looks official and relevant.

Make it contextual: Anchor security messages in the real risks your people face, using examples drawn from incidents, near misses, and reporting trends. Avoid “learnings for show”.

Ask for help: If crafting compelling messages isn’t your team’s strength, borrow talent from marketing or bring in support.

Cadence matters: Start light, then build. For a workforce new to formal security awareness, a good opening rhythm is one learning short module per month for the first six months, supported by light-touch communications and a few well-timed phishing simulations. Vary training formats to reflect different learning styles and working patterns. Keep an eye on total volume (policies, assessments, phishing, webinars) so you don’t overload people.

Always explain why — how the ISMS, policies, and processes protect customers, colleagues, and the business.

Maintaining momentum in the face of apathy

Awareness fails when it’s framed as a one-off sprint. Set expectations from day one that this is a long-term programme.

- **Build a predictable drumbeat:** Publish a 12-month calendar covering policies, education, simulations, campaigns tied to national cyber days, and internal events.

- **Create feedback loops:** Include quick polls and sentiment checks. Combine this with reporting and behavioural data to refine targeting and cadence.
- **Report visibly:** Share progress with leaders and staff (participation, phishing resilience, policy attestations, incident and reporting trends). Celebrate improvements. High reporting rates should be positioned as a sign of success — evidence of awareness, confidence, and a healthy security culture.
- **Plan the year, not the quarter:** Spend a week up front mapping assets (policies, modules, simulations, events), agreeing cadence, and lining up approvals. Then execute and review your programme regularly. This ensures awareness isn't reactive, but deliberate, coordinated, and sustainable.

Enlisting cyber security champions

Security is everyone's job, but visible allies amplify impact.

- **Identify champions** across departments; people who communicate well, spot issues early, and care about doing things right (asset owners, data owners, frontline managers).
- **Formalise an ambassador programme** with executive sponsorship and recognition.
- **Create a dedicated channel** (Teams/Slack) for updates, quick questions, and local intel.
- **Celebrate wins** (e.g., ISO 27001 recertification, phishing improvements, policy completion milestones).

Champions extend your reach, surface blind spots, and keep momentum alive between central comms.

Extending awareness to third parties

Your risk surface includes vendors, contractors, and partners. Treat them as part of the culture you're building.

Who to include

Anyone with access to your systems, data, premises, or processes should be in scope. Segment them by risk and define minimum controls per segment.

Bake it into contracts

Set expectations at onboarding: acceptable use, policy attestation, minimum education standards, and

cooperation in incident response. Make these terms part of your standard conditions and renewals.

Overcome tech hurdles

Third parties may struggle to reach on-premise tools. Provide cloud-based access to policies and learning, or an external-facing LMS/portal. Avoid paper processes for attestations.

Phase it in

Start with policy acknowledgements for highest-risk suppliers, then add targeted education (e.g., secure access, handling client data, physical security). Assess a vendor's own awareness posture during due diligence and renewals.

Keeping the load sustainable

Your users can only absorb so much. Balance quality over quantity:

- Short, focused content; relatable scenarios; plain language.
- Offer content in the languages people actually use.
- Mix formats (microlearning, videos, quick quizzes, posters/screensavers, tooltips in apps).
- Target high-risk roles (finance, privileged IT, executives) with tailored content.

Measurement that moves culture

Track what matters and act on it:

- **Participation:** completion rates, policy attestations, time-to-complete.
- **Behaviour:** phishing click/report rates, password hygiene, incident reporting quality.
- **Outcomes:** reduction in repeat incidents, audit findings closed, time to contain/respond.

Share trends with teams and leaders; set realistic improvement goals; recognise progress. Over time, these measures demonstrate whether secure behaviours are becoming embedded and where human risk is genuinely reducing.

Key takeaway

Culture change isn't a campaign you "launch and leave." It's a sustained, cross-functional effort that wins hearts and changes habits.

Start with clear intentions, keep a steady cadence, empower champions, include third parties, and measure what matters. Over time, security becomes part of how your organisation works, not just something people are told to do.

MetaCompliance

5

Chapter 5

Integrating Policy Management into Your Security Awareness Programme

Why policies matter to your security awareness

Policies turn intent into action. They make it clear what good looks like, who's accountable, and what to do in specific situations. Research shows[20] that organisations with strong policy compliance and training experience significantly fewer security incidents — in some studies up to ~50% fewer — and that most breaches stem from human error in the absence of clear standards. Without clear, accessible policies, awareness content is abstract; and staff are left guessing.

Treat policies as part of your communications system, not just documents to file away. When policies are easy to find, written in plain language, and reinforced through learning and reminders, people are far more likely to follow them.

Put policies at the heart of the campaign

Policies, education, assessments, and phishing simulations should work **as one coordinated plan**. Run them separately and you risk flooding inboxes, diluting focus, and missing behaviour change.

Anchor your campaign to a few core ideas:

- **One source of truth:** A central, searchable policy hub that everyone can access.
- **Plain language:** Short, role-relevant policies with clear do/don't examples.
- **Accountability:** Named owners, clear review cycles, and version history.
- **Evidence:** Digital attestations, timestamps, and an audit trail for regulators.

Design a simple policy communication plan

Before publishing, decide who needs what, when, and why. A lightweight plan should cover:

- **Audience & segmentation:** Roles, locations, languages, employment types and third parties in scope.
- **Messages & mediums:** Email, LMS notification, manager cascades, Teams/Slack posts, screensavers/posters.
- **Timing & cadence:** Launch dates, reminders, recertification dates, audits or peak risk periods.
- **Education linkage:** Which microlearning or simulation reinforces this policy.
- **Governance:** Policy owner, approver, next review date, and change-control steps.
- **Measurement:** Completion and attestation rates, quiz results, incident trends linked to the policy topic.

Educate to the policy (don't just retell it)

Policies exist to mitigate defined risks. Your education modules should:

- Focus on the behaviours that matter most (e.g., reporting, data handling, approvals).
- Use scenarios and quick decision-points, not verbatim summaries.

- Include a check-for-understanding (short quiz or click-through decision tree).
- Point back to the policy for detail ("Learn more / full procedure").

High-risk areas (e.g., privileged access, payments, incident response) may need a hybrid approach: policy + microlearning + short live briefing.

Onboarding without overload

New starters are absorbing a lot. Make learning progressive and human:

- **Week 1:** Essentials only (acceptable use, password & MFA, phishing basics, incident reporting).
- **Weeks 2–4:** Add role-specific policies (data handling for Finance/HR, device use for field teams, supplier access for Procurement).
- **Guardrails:** Cap eLearning to ~3 hours per week in Month 1; shift to just-in-time nudges thereafter.
- **Manager role:** Use short checklists to confirm key behaviours are understood and in place.

Build a centralised policy management system

Manual spreadsheets and file shares can't keep up. A central platform should provide:

- **End-to-end lifecycle:** Draft → review → approve → publish → retire, with version control.
- **Targeting & access:** Segment by role, location, language, employment type, and vendor; mobile-friendly access.
- **Attestation & reminders:** Digital sign-off, automated nudges, escalation paths, and re-certification windows.
- **Education links:** Associate each policy with the right learning object(s) and phishing templates.
- **Reporting:** Real-time dashboards for completion, exceptions, and overdue items; exportable audit packs.
- **Integrity:** Tamper-evident storage for evidential weight in investigations or legal disputes.

Aim for near-100% attestation on mandatory policies. Use automation to close gaps, and escalate thoughtfully (manager nudges before HR).

Who uses the system (and how)

Manual spreadsheets and file shares can't keep up. A central platform should provide:

- **Administrators:** Configure lifecycle workflows, publish policies, target audiences, schedule recertification, and map related learnings.
- **Employees & contractors:** Access a clean, searchable hub; complete attestations; revisit policies when needed; choose their preferred language.
- **Leaders, auditors, regulators:** View dashboards, evidence packs, and change history to confirm duty of care and oversight.

Connect policies to frameworks and regulation

Well-run policy management supports ISO/IEC 27001:2022 (clauses 5, 7.2–7.5, 8, and 9 on governance, competence, communication, and documented information) and aligns naturally with the NIST CSF 2.0 Govern function. In regulated sectors, strong policy governance helps demonstrate security-by-design and operational resilience (e.g., GDPR obligations; DORA principles for financial entities and ICT providers).

Make culture the outcome

Policies change culture when they're:

- **Relevant** (tailored to real risks and roles),
- **Reachable** (easy to find and understand), and
- **Reinforced** (through education, manager conversations, simulations, and timely reminders).

Measure not just completion, but behavioural signals: fewer repeat incidents, faster reporting, better phishing resilience, and cleaner audit findings.

Key takeaway

Policy management is how you operationalise security.

Centralise it, simplify it, and thread it through your awareness programme so people always know what “good” looks like, and can prove they’re doing it.

MetaCompliance

6

Chapter 6

Developing a Best-Practice Cyber Awareness Strategy

Start with a realistic plan you can actually manage

Cyber security awareness works like any other business programme.

It requires:

- Clear objectives
- Executive sponsorship
- A 12-month plan
- Measurable outcomes

Your strategy should align:

- People
- Policy
- Process
- Technology

It should also be designed to fit into day-to-day operations, making it simple for busy teams to do the right thing, follow secure practices, and recognise potential risks before they become real incidents.

Secure visible executive support

Leadership backing determines resourcing, momentum, and tone.

Make it concrete:

- **Kick-off message from the top** (short email/video) setting expectations and the "why".
- **Decision points agreed up front:** escalation paths for persistent non-completion, response to repeated phishing failures, how exceptions are handled.
- **Leader enablement:** a 60–90 minute executive briefing plus a short executive-level eLearning module.
- **Quarterly review slot** on the governance agenda for results and risks.

Leaders model behaviour. If they complete their modules on time, talk about it, and ask for the metrics, everyone else follows.

Build the campaign plan

Create a 12-month, cyber risk-focused calendar that your team can realistically deliver alongside their existing responsibilities.

Core components to schedule:

- **Kick-off message from the top Policies:** publication/recertification windows with clear owners.
- **Education:** microlearning (5–10 mins), targeted role modules, and manager talking points.
- **Simulated phishing:** varied scenarios, measured fairly, with just-in-time coaching.
- **Comms:** monthly themes, internal posts, posters/screensavers, tooltips.
- **Surveys/assessments:** short pulse checks to gauge understanding and sentiment.
- **Moments:** align with audits, product launches, peak scam seasons, national cyber days.

Cadence guidance: favour little and often. For most organisations, 1–2 core touchpoints per month plus light nudges keeps attention high without fatigue.

Establish a baseline

You can't improve what you don't measure. Capture the current state of phishing, policy coverage and knowledge, then re-measure on a regular rhythm.

Quick baseline methods:

- **Incident look-back (12 months):** cluster by cause (phishing, mis-send, misconfiguration, lost device, access error).
- **Simulated phish:** initial click rate, credential-submit rate, and report rate.
- **Policy health:** list top policies, last review date, current attestation coverage.
- **Knowledge pulse:** 8–12 question survey tied to your top risks (keep it under 3 minutes).

Document the baseline and share it with sponsors so success criteria are agreed early.

Define success and track it

Choose a focused set of KPIs that reflect **behaviour change and outcomes**, not just activity.

- **Participation:** module completion %, time-to-complete; policy attestation coverage and ageing.
- **Phishing resilience:** click %, credential-submit %, and report rate (aim to move report rate up over time).
- **Incident trends:** repeat incidents per category, mean-time-to-report (MTTR), and mean-time-to-contain (MTTC).
- **Third-party assurance:** % of in-scope vendors with policy attestation and completed awareness.
- Sentiment/understanding: quarterly pulse survey on "I know what to do if…".

Target style: set realistic quarter-on-quarter improvements (e.g., -25% relative phish clicks, +30% report rate, 95%+ policy attestation within 21 days).

Report monthly to the programme owner and quarterly to governance/board. Highlight wins, blockers, and next experiments.

Use a hybrid approach (because one channel won't cut it)

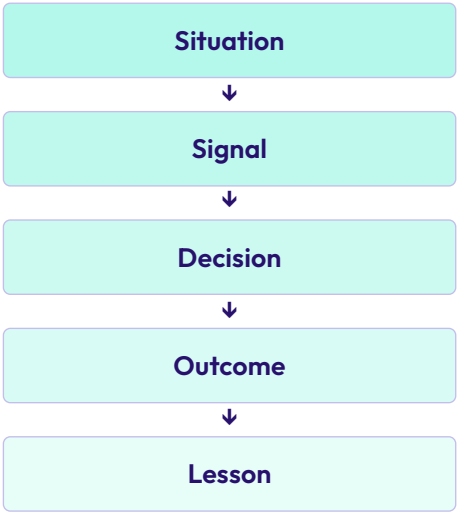
Different people absorb information in different ways. Mix channels to keep messages fresh and reach everyone:

- **Microlearning:** short, scenario-based, role-relevant; close with a single action ("Next time: hover, verify, report").
- **Manager moments:** 3–5 minute team huddles with a one-pager and two discussion prompts.
- **Simulations:** email, SMS, collaboration-app lures; rotate difficulty and themes.
- **Visuals:** posters, screensavers, short loops on office displays tied to monthly risks.
- **Just-in-time nudges:** contextual reminders in apps (e.g., large external recipient list, file-sharing outside domain).
- **Stories:** short internal case studies or anonymised near-misses — what happened, what helped, what we changed.

Keep the tone respectful, human, and practical. Avoid shaming; focus on learning and enabling quick recovery from mistakes or near-miss incidents.

Tell better stories

Stories beat statistics for memory and action. Frame communications with a simple arc:



Example:

"A supplier emailed Accounts with an urgent bank change (situation). The sort code was new and the message asked for secrecy (signals). The analyst called the known contact to verify (decision). Payment was protected (outcome). Always verify out-of-band for payment changes (lesson)."

Automate where it helps

Automation prevents drift and preserves your team's energy for high-value work.

Automate:

- **Targeting and delivery** of policies and education by role, location, language, start date.
- **Reminders and escalations** (polite → manager → HR, as appropriate).
- **Recertification windows** (annual/biannual).
- **Evidence packs** for audits (attestations, versions, completion logs).
- **Dashboards** for leaders and auditors.

Keep human oversight for content quality, tone, exceptions, and post-incident reviews.

Who runs what (and how you'll staff it)

A small, cross-functional core team works best:

- **Programme lead (IS/Privacy):** owns risk alignment, roadmap, KPIs.
- **Comms/Marketing partner:** crafts messages, visual assets, themes.
- **L&D/eLearning specialist:** designs learning objects and assessments.
- **Security ops liaison:** feeds live threat intel and incident learnings into monthly themes.
- **HR/People partner:** aligns with onboarding, manager enablement, and performance processes.
- **Regional/Language reps:** localise copy and context.

Meet monthly; publish the calendar; iterate quarterly.

Pulling it together: your first 90 days

New starters are absorbing a lot. Make learning progressive and human:

Days 1–30

↓

Confirm executive sponsor and success metrics

Baseline: incidents, policies, phish, pulse survey

Build the 12-month calendar and asset list

Days 31–60

↓

Publish policy hub refresh and target two mandatory policies

Launch first microlearning + simulation + poster set on a single security theme

Stand up dashboards; brief managers

Days 61–90

↓

Review results; tune targeting and difficulty

Launch champions network and comms channel

Present Q1 outcomes to leadership; agree next quarter's focus

Key takeaway

Effective awareness programmes aren't louder; they're smarter, sponsored from the top, paced over a year, measured on behaviour, and delivered through a mix of targeted content, manager conversations, and smart automation.

Do that consistently, and you'll see culture and risk move in the right direction.

MetaCompliance

7

Chapter 7

Ten Cyber Security Awareness Best Practices

These ten best practices will help you build an awareness programme that drives genuine behaviour change, as well as compliance.

1. **Start with visible CEO leadership**
2. **Know your organisational risk tolerance**
3. **Defend your information assets**
4. **Focus on high-risk groups — and how they learn**
5. **Make it engaging with storytelling**
6. **Keep policy management current and connected**
7. **Prepare for a data breach before it happens**
8. **Enlist cyber security champions**
9. **Assess and secure your supply chain**
10. **Implement oversight and continuous improvement**

1 Start with visible CEO leadership

Cyber security culture is set at the top. When the CEO champions awareness and models good practice, it reframes security as a business priority, not an IT initiative.

An engaged CEO:

- Signals that security is a business priority, not an IT task.
- Helps allocate resources and remove barriers.
- Reinforces accountability through their own participation.

Kick off each campaign with a message or short video from the CEO explaining why awareness matters and how everyone contributes to protecting the organisation's reputation, customers, and data.

2 Know your organisational risk tolerance

Before planning campaigns, understand your threat landscape and risk appetite.

Define what level of risk is acceptable and where you draw the line. This means education and communications focus on realistic, high-impact threats, not hypothetical ones.

To stay aligned:

- Conduct regular risk assessments mapped to frameworks such as **ISO/IEC 27001, NIST CSF 2.0**, and **GDPR** requirements.
- Review emerging regulations (like DORA in the EU for financial institutions and ICT providers) to ensure awareness efforts support compliance.
- Revisit risks quarterly — technology, vendors, and threats evolve quickly.

3 Defend your information assets

You can't protect what you don't know exists. Start with a full inventory of your information assets, from customer data to internal IP.

For each asset:

- Classify it (public, internal, confidential).
- Identify who owns it and who can access it.
- Map how it's stored, processed, and transmitted.

Once you know where your most valuable data lives, awareness efforts can focus on the human behaviours that matter most: safe handling, secure sharing, and reporting anomalies.

4 Focus on high-risk groups — and how they learn

Not all roles face the same risks, and not all people learn in the same way. Effective programmes target both.

High-risk groups often include:

- **Finance teams** — exposed to payment fraud, BEC, and AI-enabled impersonation
- **HR** — handle sensitive personal and employment data
- **Executives** — authority, visibility, and access make them prime targets
- **Privileged IT users** — configuration, automation, and access errors can escalate quickly

Targeting means more than different content — it means different formats and reinforcement:

- Scenario-based microlearning for operational teams
- Short decision prompts and checklists for time-poor leaders
- Hands-on simulations or briefings for technical users

Use incident data, assessments, phishing results, and reporting trends to prioritise where effort will reduce risk most.

5 Make it engaging with storytelling

People remember stories, not slides. Bring security to life through narratives, humour, and relatable scenarios.

Use storytelling to:

- Illustrate cause and effect ("This small click led to a £50k loss").
- Show real people making smart choices.
- Frame employees as heroes defending the business, not potential liabilities.

Keep stories authentic; draw from real incidents, anonymised examples, or themed campaigns (for example, a "Mission: Secure" storyline).

6 Keep policy management current and connected

Policies are the rulebook that keeps everyone aligned. Outdated or hard-to-find policies quickly erode compliance and trust.

An effective policy management system should:

- Maintain one **central, searchable hub.**
- Include **automated version control**, approval workflows, and digital attestations.
- Link each policy to relevant education or eLearning.
- Provide dashboards to track completion and renewal cycles.

Regularly review policies alongside your awareness plan to ensure messaging, controls, and regulatory needs stay in sync.

7 Prepare for a data breach before it happens

Incidents are inevitable. The difference between a crisis and a controlled response lies in preparation.

Build and test an incident response plan that defines:

- Roles and responsibilities for all key teams.
- Communication protocols (internal, customer, regulator).
- Escalation paths and backup decision-makers.

Rehearse with tabletop exercises. Each test should identify gaps and end with an updated playbook.

Awareness tip: run a "breach simulation" communication exercise as part of your education modules and walk staff through how the organisation would respond.

8 Enlist cyber security champions

Champions amplify awareness and humanise security. They're not necessarily technical experts but engaged employees who model good practice and influence peers.

To make it work:

- Recruit from diverse departments and regions.
- Give champions early access to content and key messages.
- Recognise contributions publicly and celebrate milestones (like phishing resilience improvements or ISO recertification).

Champions create local ownership and provide an early-warning system for fatigue or confusion.

9 Assess and secure your supply chain

Your security is only as strong as your least-secure supplier.

Supply chains are common attack routes, often exploited through weak controls or outdated systems. Research shows[21] that over half of cyber security incidents involve the supply chain, with attackers targeting third-party vendors and services to compromise larger organisations. Business should build third-party awareness and assurance into contracts and onboarding to reduce this risk.

Best practice includes:

- Performing due diligence and regular vendor risk assessments.
- Requiring policy acknowledgement and minimal awareness education for anyone accessing your systems or data.
- Segmenting suppliers by risk level and applying appropriate controls.
- Tracking completion and compliance via your policy management system.

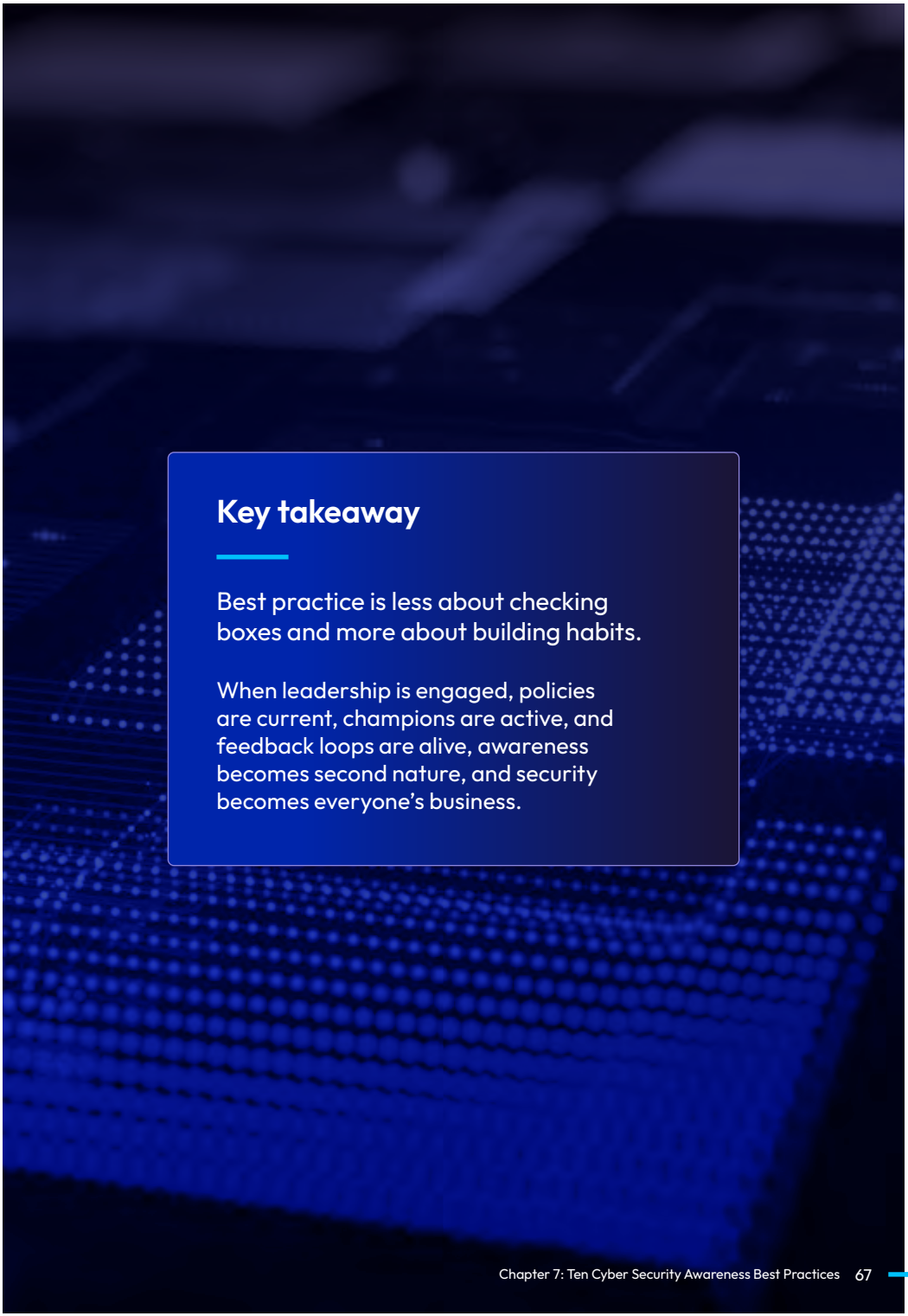
10 Implement oversight and continuous improvement

Cyber awareness is never "done." Threats, tools, and people all change, and your programme must evolve with them.

Establish a simple review rhythm:

- Quarterly: update metrics, analyse incidents, and adjust campaign themes.
- Annually: conduct a full programme review, including policy updates, risk re-evaluation, and new content planning.
- After every incident: feed lessons learned back into education and simulation design.

Document everything — metrics, lessons, updates — to demonstrate due diligence and regulatory compliance.



Key takeaway

Best practice is less about checking boxes and more about building habits.

When leadership is engaged, policies are current, champions are active, and feedback loops are alive, awareness becomes second nature, and security becomes everyone's business.


MetaCompliance

About MetaCompliance

The UK's Leading Human Risk Management Provider

MetaCompliance is the human risk management company transforming how organisations build resilient security cultures. Our intelligent enterprise-ready platform combines personalised cyber security education, behavioural analytics, and automation to measure, mitigate and manage human risk at scale. Trusted by over six million users worldwide, we help global enterprises reduce risk and embed lasting behaviour change.

Built for the way people learn and work

Our platform is designed around how people actually learn— short, visual, interactive, and relevant to their role. It's flexible and scalable, so you can tailor every element to your brand, policies, and workforce.

With fresh content created every month by our in-house team, including live-action videos, avatars, microlearning, and quizzes, you'll always have new ways to keep awareness alive.

Everything lives in one place, available in 44+ languages, delivered through an intuitive platform that saves time, reduces risk, and supports compliance; all backed by real experts who are always on hand to help.

Why organisations choose MetaCompliance

- **European market leader** in human risk management and security awareness.
- **Proven results** — reducing risk and building security-first cultures at scale.
- **Comprehensive platform** — policies, phishing, education, analytics, and reporting in one place.
- **People-first approach** — designed for engagement, not just compliance.
- **Continuous innovation** — evolving as fast as the threats you face.

Find out more at www.metacompliance.com

References

1. Special Report: Cyberwarfare In The C-Suite, Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025

2. Business Insights, Bitdefender, Human error identified as the #1 reason behind most cyberattacks

3. Verizon 2025 Data Breach Investigations Report, Verizon Business, 2025 Data Breach Investigations Report | Verizon

4. Ransomware Roundup, Industrial Cyber, Global ransomware attacks rose 32% in 2025, as manufacturers emerged as top target - Industrial Cyber

5. Special Report: Cyberwarfare In The C-Suite, Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025

6. ISO/IEC 27001:2022, ISO, ISO/IEC 27001:2022 - Information security management systems

7. National Institute of Standards and Technology (2024) The NIST Cyber Security Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cyber Security White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

8. GDPR, Intersoft Consulting, General Data Protection Regulation (GDPR) – Legal Text

9. Digital Operational Resilience Act (DORA), European Insurance and Occupational Pensions Authority, Digital Operational Resilience Act (DORA) - European Insurance and Occupational Pensions Authority

10. The EU Artificial Intelligence Act, EU Artificial Intelligence Act, EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act

11. Document 32022L2555, Official Journal of the European Union, EUR-Lex, Directive - 2022/2555 - EN - EUR-Lex

12. Cyber Resilience Act, European Commission, Cyber Resilience Act | Shaping Europe's digital future

13. Cyber Security and Resilience Bill, GOV.UK Cyber Security and Resilience Bill - GOV.UK

14. Cyber Security Framework, NIST, Cyber Security Framework | NIST

15. Microsoft Digital Defense Report 2025, Micosoft, cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/security/Microsoft-Digital-Defense-Report-2025.pdf

16. Finance worker pays out $25 million after video call with deepfake 'chief financial officer', CNN World, Finance worker pays out $25 million after video call with deepfake 'chief financial officer' | CNN

17. Security training cuts phishing risk by 86% globally in a year, Security Brief, https://securitybrief.news/story/security-training-cuts-phishing-risk-by-86-globally-in-a-year

18. PwC's 2025 Global Digital Trust Insights Survey, PWC, Only 2% of businesses have implemented firm-wide cyber resilience, even as cyber security concerns are top-of-mind and the average data breach exceeds US$3M: PwC 2025 Global Digital Trust Insights | PwC

19. Data Breach Statistics 2025: Costs, Causes, Trends, and Insights, Deepstrike, Data Breach Statistics 2025: Global Costs and Trends

20. The Importance of Policy Compliance Management in Strengthening Cyber Security, moldstud, Strengthening Cyber Security through Policy Compliance Management | MoldStud

21. Global Third Party Breach Report, Security Scorecard, Global Third Party Breach Report - SecurityScorecard

MetaCompliance

www.metacompliance.com