Mind Science

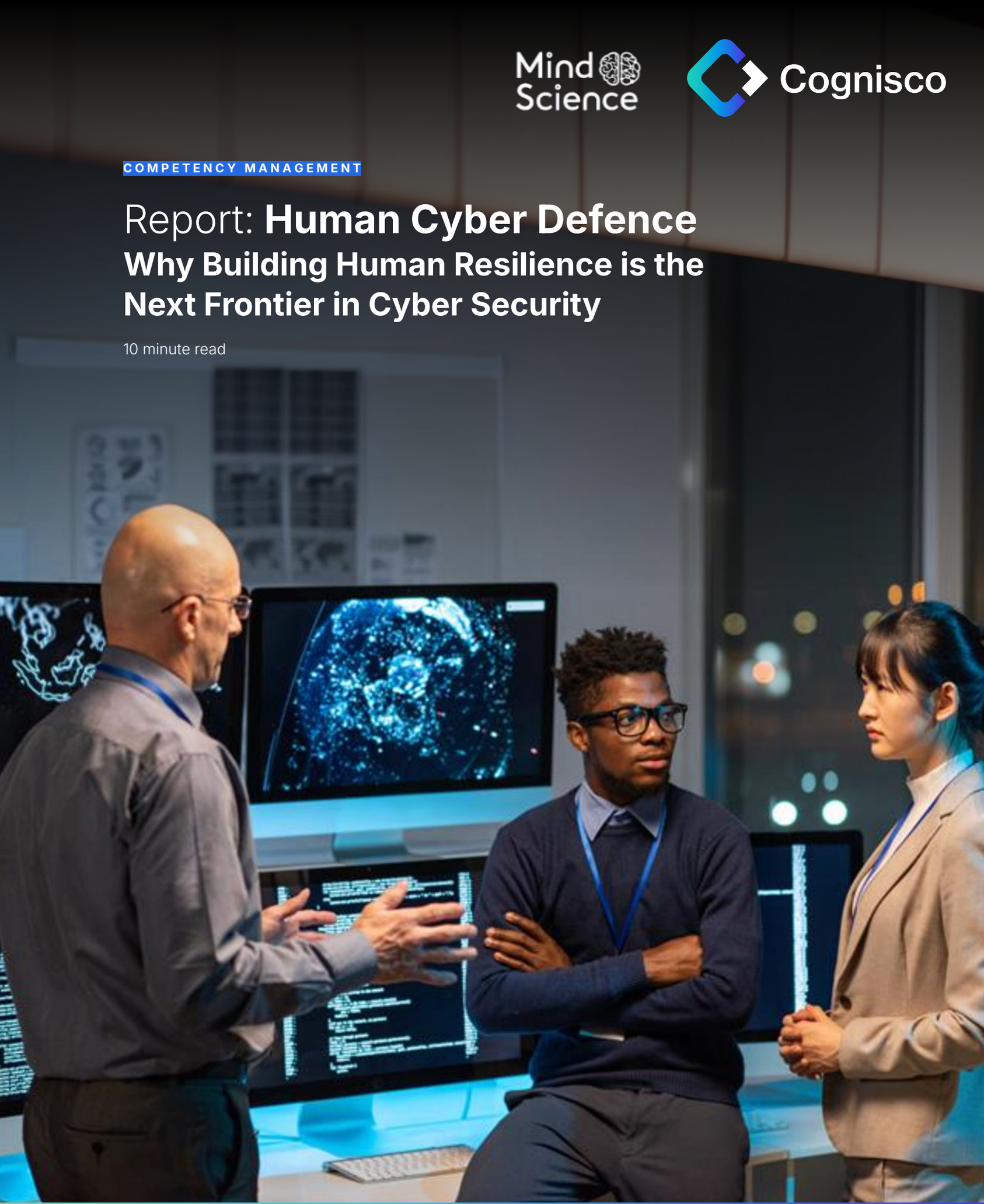
Cognisco

COMPETENCY MANAGEMENT

Report: **Human Cyber Defence**

Why Building Human Resilience is the Next Frontier in Cyber Security

10 minute read



Foreword

In an era where cyberattacks are not only more frequent but more sophisticated, organisations are investing heavily in digital infrastructure and technical security systems. Yet, even with best-in-class technology, the weakest point in most organisations remains the same: people.

At **Cognisco**, we believe that empowering people, not blaming them, is the key to sustainable cybersecurity. This white paper explores how organisations can build human cyber resilience by combining psychological insight, situational judgement and a strong cultural foundation.

Drawing on insights from our recent webinar, **Building Human Resilience in Cyber Security Environments**, co-hosted with **human science expert Bec McKeown** from **Mind Science**, this report dives into the challenges and opportunities facing businesses in tackling cyber threats from the human angle.

Social Engineering accounts for approximately **70–90%** of cyber attacks, with **phishing** being the most prevalent method

Source: Secureframe, 2025

Introduction

1. Cybersecurity's Hidden Weakness and Strength

For many years, the dominant narrative in cybersecurity has focused on firewalls, encryption, antivirus software, and cloud security. Yet research consistently shows that most cyber incidents involve human error.

Whether it's a phishing email opened by a junior employee or a missed software patch by a system admin, human actions, or inactions, are the tipping point for most breaches.

But herein lies the opportunity: if people are the most common vulnerability, they can also become the most powerful defence, if properly trained, supported and psychologically equipped.

Cyber defence is no longer just about systems, it's about people.

95%

of cyber incidents involve human error

IBM - 2024

Understanding the Human Dimension of Cyber Risk

Cybersecurity often assumes people are either a risk or a nuisance: “the weakest link.” This oversimplifies a deeply complex reality. People are capable of navigating high-pressure, ambiguous situations, when they have the tools and support to do so.

2.1 The Myth of the ‘Weakest Link’

Bec McKeown (Mind Science) challenges this myth:

“Calling humans the weakest link is not only unhelpful, it’s damaging. It creates a culture of blame rather than learning. We need to talk about people as the first line of defence, not the last resort.”

2.2 Where Human Risk Appears

Phishing Attacks: 91% of successful cyber attacks begin with a phishing email. Even experienced employees can fall victim under stress or distraction.

Password Hygiene: Despite awareness, people still reuse weak passwords, a behaviour driven more by overload than ignorance.

Misconfigured Systems: Cloud environments offer power and flexibility, but the human configuration behind them introduces risk.

Poor Crisis Handling: Even with excellent incident response plans, employees may freeze or make misjudgements during a real attack.

Why Cyber Resilience Requires a Human Focus

Modern cyber threats exploit more than technical vulnerabilities, they exploit **human psychology**: fear, distraction, overload and uncertainty.

3.1 Stress and Decision-Making

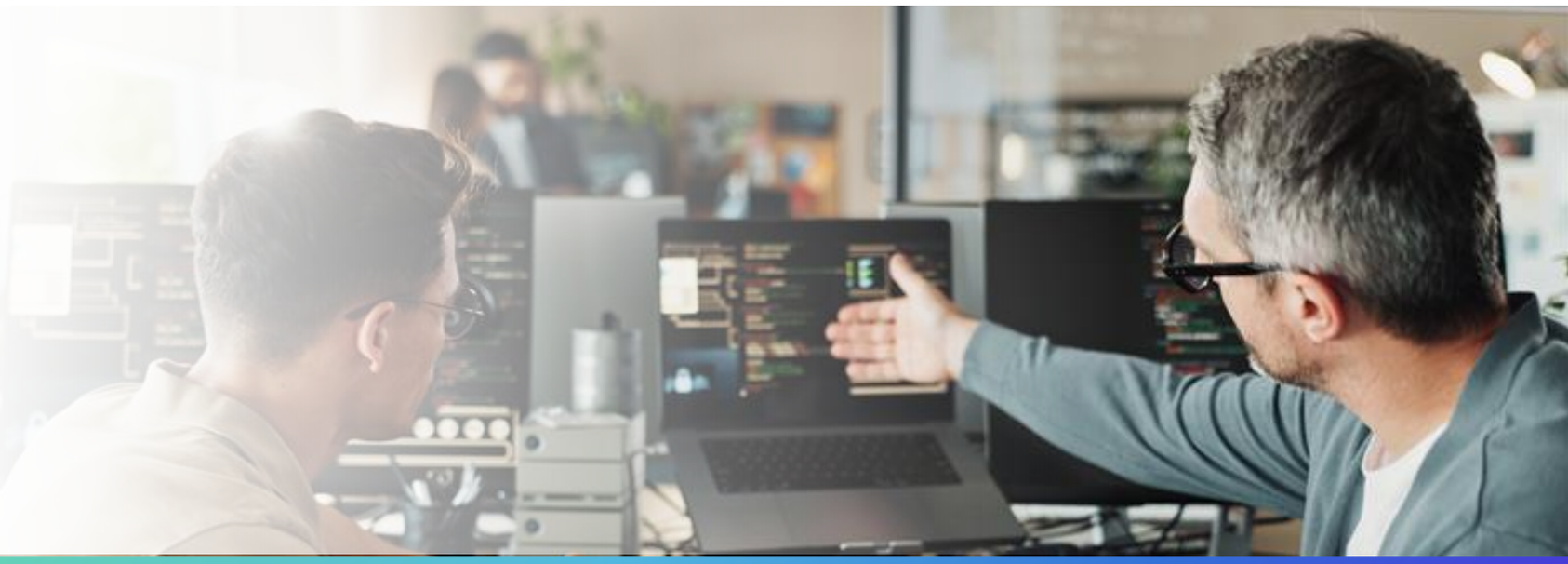
High-stress situations such as live cyber incidents trigger our fight-or-flight response. This can lead to:

- **Tunnel vision**: focusing only on what's directly in front of us.
- **Cognitive narrowing**: losing sight of the bigger picture.
- **Decision paralysis**: being unable to act due to fear of blame.

3.2 Cognitive Biases in Play

- **Anchoring**: Fixating on the first information received.
- **Confirmation bias**: Seeking out information that confirms our assumptions.
- **Groupthink**: Suppressing doubt in the face of consensus.

In cyber incidents, these mental shortcuts can dramatically increase response time, or lead to catastrophic missteps.



What Is Human Cyber Resilience?

4. Human Cyber Resilience

Human Cyber Resilience is the ability of individuals and teams to **perform effectively under pressure during cyber incidents**, making sound decisions, communicating clearly and adapting to uncertainty in real time.

While traditional cybersecurity focuses on technology and process, human cyber resilience focuses on **how people think, behave and respond** in dynamic and often ambiguous situations.

Mind Science has identified that **Cognitive Readiness** is imperative and provides training to develop teams on the cornerstone principles below. Cognisco, in partnership with **Mind Science,** have developed a diagnostic tool to help organisations measure, understand and enhance resilience within their teams, closing the gap between human behaviour and cyber defence.

The Adaptive Mindset

To be self-aware, continuous learners. Able to work cohesively in groups of people with different skills, personalities and expertise.

Agile Thinking Skills

Techniques and strategies to identify and evaluate problems and apply critical reasoning to implement appropriate response strategies.

Agile People Skills

Enhance performance by understanding what behaviours and skills to leverage and which to minimise depending on the nuances of the situation.

Agile Team Skills

Build high-performing teams and make practical changes to get teams working together in a psychologically safe environment.

What Is Human Cyber Resilience?

4. Human Cyber Resilience

It involves three core capabilities:

a. Cognitive Readiness

This is the mental preparedness to respond to unexpected situations, including situational awareness, pattern recognition and agile thinking. Cognitive readiness enables people to assess evolving threats and act, even when data is incomplete or rapidly changing.

b. Emotional Control

Cyber incidents often involve high stakes, high stress and time pressure. Emotional resilience allows individuals to remain calm, regulate their responses and avoid panic-driven or overly cautious behaviours. Teams perform better when individuals can manage stress and support others during tense situations.

c. Behavioural Confidence

People may know what to do, but hesitate if they lack confidence. Building confidence through realistic training, simulations, and scenario-based assessment is key to ensuring people act (not freeze) when it matters most.

Human cyber resilience complements, not replaces, technical systems. Technology may detect a breach, but people decide how to respond, how to communicate and how to lead the recovery effort. Organisations that invest in human resilience are not only safer but also more adaptable, collaborative and trusted.

Human Cyber Resilience is not just about knowledge, it's knowing what to do when the situation doesn't match the textbook.

Tools to Assess and Build Human Cyber Resilience

5.1 Situational Judgement Testing (SJT) with Confidence Ratings

Cognisco's approach includes SJTs tailored to cybersecurity roles. These tests:

- Simulate **real-world** cyber incident scenarios
- Measure both **correctness of decisions** and **confidence** in those decisions
- Highlight gaps between **perceived** and **actual competence**

This is crucial for identifying:

- Hidden risk areas
- Overconfidence in key roles
- Training needs across departments

People may know what to do in theory, but do they feel confident enough to act under pressure?

5.2 Targeted Training That Builds Agility

Effective training goes beyond awareness videos. It includes:

- Scenario-based learning
- Interactive crisis simulations
- Peer collaboration exercises
- Feedback loops that build self-awareness

5.3 Psychological Profiling and Role Suitability

Some roles in cybersecurity require high tolerance for ambiguity, rapid information processing and emotional control. Understanding individual strengths and limits can help assign roles more effectively, or design appropriate support systems.

Organisational Culture: The Bedrock of Cyber Resilience

No amount of training can compensate for a poor culture, where **fear of blame, lack of psychological safety, or siloed thinking** undermine even the best-prepared teams. Without the right environment, people may hesitate to report issues, delay decisions, or avoid taking responsibility — all of which can escalate the impact of a cyber incident.

6.1 Just Culture vs. Blame Culture

In a **blame** culture:

- Mistakes are hidden
- Reporting is delayed
- Employees operate defensively

In a **just** culture:

- Errors are learning opportunities
- Transparency is encouraged
- Employees act proactively

A cyber breach doesn't have to be catastrophic, but poor internal handling often turns it into one.

65% of employees admit to bypassing their organisation's cybersecurity policies, often to enhance productivity

Source: Medium, 2024

6.2 The Importance of Psychological Safety

Research shows that teams with higher psychological safety:

- Make faster decisions
- Communicate more openly
- Report incidents more rapidly
- Are less likely to freeze under pressure

Psychological safety is the fuel for fast, decisive, and responsible action in a cyber crisis.

Cross-Functional Collaboration in Incident Response

Cybersecurity is no longer the sole domain of IT departments. Today's cyber threats require **a coordinated response across multiple business functions**, each playing a distinct but interdependent role. Without this cross-functional alignment, even the most robust technical defences can be undermined by confusion, delays, or competing priorities during a live incident.

7.1 Key functions in cyber incident response include:

- **IT & Security**: Leading technical containment, investigation and recovery.
- **Legal & Compliance**: Managing regulatory notifications, data protection requirements and liability.
- **Communications & PR**: Shaping internal and external messaging to protect trust and reputation.
- **HR & Learning**: Supporting staff under stress, identifying training needs and managing internal reporting culture.
- **Executive Leadership**: Making time-critical strategic decisions that may involve legal, operational and reputational trade-offs.

7.2 Why collaboration matters

In a high-pressure cyber crisis, **misalignment between teams can cause delays, duplicated effort, or contradictory actions**. For example, comms may downplay an incident while IT escalates it internally, causing confusion and potential reputational damage.

The last thing you need in a crisis is for your teams to be fighting over priorities instead of working toward resolution. True cyber resilience requires:

- Pre-defined roles and responsibilities
- Regular joint simulations and tabletop exercises
- Shared understanding of protocols and escalation paths
- A culture of mutual respect and open communication

Organisations that foster collaboration before an incident occurs are significantly better equipped to respond quickly, coherently and effectively when the real thing hits.

Communicating During a Cyber Crisis

How an organisation communicates during a crisis can make or break its reputation, as many who have been hit in recent years can attest to.

Do:

★Communicate early, even if you don't have all the answers
★Be honest about what's known and what's being done
★Reassure stakeholders and customers about response steps

Don't:

★Attempt to cover up
★Minimise the severity
★Delay disclosures out of fear

In a cyber crisis, how you communicate is just as important as what happened, transparency builds trust, while silence breeds suspicion.

Recent examples: What can we learn?

HSE Ireland (2021)

- A ransomware attack overwhelmed systems and personnel
- Despite technical defences, response teams lacked cognitive readiness
- Delays in response worsened outcomes

Equifax (2017)

- A known vulnerability went unpatched
- Poor communication worsened public perception
- Highlights need for accountability, agility and leadership

NHS Trust (2023)

- A single point of failure led to system shutdown
- Teams scrambled without cross-department coordination
- Emphasises importance of real-time decision-making under pressure

CONSTRUCTION AND UTILITIES

Building Human Cyber Resilience

1. **Conduct a human-centric risk assessment:**
   Include confidence ratings, not just compliance checks.
2. **Implement Situational Judgement Testing:**
   Use realistic cyber scenarios to test decision-making.
3. **Train cognitive and emotional skills:**
   Develop metacognition, stress management and critical thinking.
4. **Create a culture of psychological safety:**
   Enable fast reporting, cross-functional alignment and open dialogue.
5. **Practice, simulate, and review:**
   Use live simulations and tabletop exercises to prepare teams.
6. **Align leadership and communications:**
   Build unified messaging protocols for internal and external use.

Conclusion: The Future of Cybersecurity Is Human

As the digital threat landscape evolves, so must our response. While firewalls, encryption, and AI detection tools are essential, they are not sufficient. People are the true frontline of cyber defence.

By developing human resilience through training, culture and cognitive readiness, organisations can create a flexible, fast and confident cyber response capability.

In cyber security, the best defence isn't just smart systems. It's smart people.

How Cognisco can help

To address the human challenges at the heart of cybersecurity, Cognisco has developed a **Human Cyber Defence Assessment** in our behavioural and skills diagnostic tool MyKnow 365, designed to evaluate an organisation's real-world cyber readiness at an individual and team level.

This unique assessment goes beyond technical knowledge, focusing on how people behave and make decisions under pressure. It evaluates:

- **Cybersecurity Awareness and Risk Behaviour**
  Understanding of cyber threats, secure practices and vulnerability to social engineering.
- **Regulatory and Compliance Confidence**
  Ability to apply compliance knowledge in high-stress, real-time scenarios, not just recall it.
- **Leadership and Communication Under Pressure**
  How team leaders guide, inform, and support their teams during incidents or near misses.
- **Crisis Decision-Making and Judgement**
  The capacity to make sound, timely decisions in ambiguous or fast-moving cyber situations.

Benefits of the Assessment:

- **Identify Gaps in Human-Centric Cyber Readiness**
  Pinpoint individuals or roles where low confidence or behavioural risk may compromise response effectiveness.
- **Strengthen Organisational Resilience and Response**
  Ensure that staff at all levels are not only trained but ready and equipped to respond collaboratively.
- **Develop Targeted Training and Support Plans**
  Build structured, role-specific development programmes based on real diagnostic data, not assumptions.

About Cognisco

Cognisco understands that training alone is not enough to evidence a competent and confident workforce.

We have over 25 years' experience working with organisations to identify what every employee needs to know, do and understand to do their job competently and confidently and to mitigate risk.

Our behavioural and skills diagnostic, MyKnow 365, provides enhanced competency assurance by verifying that each individual has the necessary competencies, training and certification, supporting robust scheduling and due diligence.

This helps organisations measure, manage and monitor competency and capability across their workforce frameworks.

We work with some of the world's largest and most complex organisations including **The NHS, National Rail, His Majesty's Civil Service, John Lewis** and some of the UK's leading construction and utility providers.

Mitigating risk. Maximising people potential.

Get in touch

Krishna Williams
Business and Channel Development Manager
kwilliams@cognisco.com
+44 (0)7570 685645