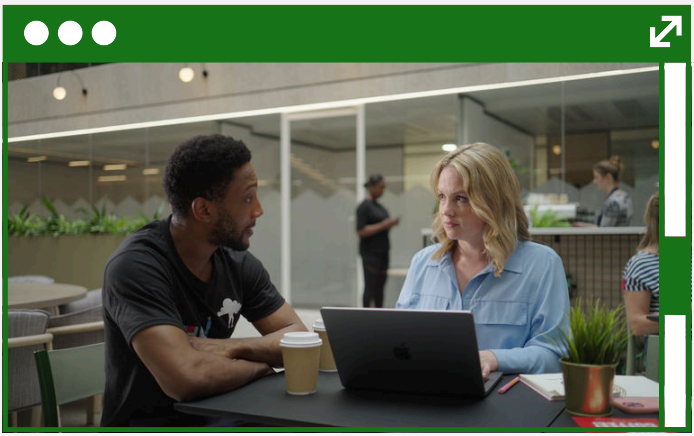
video arts™
Longer lasting learning

Cyber-Smart Leadership

5 Skills Every Leader Needs to Keep Their Team and Organisation Safe

Table of Contents

Introduction



Cyber threats, like most things with a digital pulse, tend to land squarely in the IT department's inbox. From firewalls to encryption, the tech team are the go-to defender of digital safety. But we cannot leave it all to them; at the end of the day, **they are only human.**

Likewise, we cannot simply rely on the tech either. Research shows that **74% of breaches involve some form of human error**[1]; the problem rarely lies with the technology itself. It lies in how it is used, misused, or ignored entirely by actual humans.

This is why leadership matters. A growing body of research shows that when managers actively support good cyber habits, teams are significantly more likely to follow them[2].

You do not need to be a cybersecurity expert. But you do need to champion awareness, model best practices, and create a culture where it is safe to ask questions and admit mistakes.

In this eBook, we will explore five essential leadership skills that can transform how teams respond to cyber threats. Whether you are dealing with prevention, action, or recovery, these skills will help you guide your team safely through it all.

Why Trust Us?

video arts™
Longer lasting learning

We may not be the ones configuring firewalls or updating antivirus software, but we know what makes best practices stick...

At **Video Arts**, we help people build habits that make a difference. With over 50 years of experience in behaviour-led learning, we understand how to help teams remember what matters and act on it when it counts.

On top of that, we've just launched some new **Cyber Security courses** that are built in collaboration with **subject matter experts,** so you get the right information, backed by the people who know their stuff. But more importantly, the courses are delivered in the **Video Arts** way.

That means:

- **Human-first content** that resonates with real teams
- Actually funny (yes, even in cyber security)
- **A Learning Library** featuring over **400 courses**, organised into **9 collections** covering all key areas of workplace Learning & Development.
- Our courses are designed to **embed real change**, not just to tick a compliance box

More than just e-learning, these are tools that help leaders create a culture of awareness, responsibility and confidence.

Skill One: Curiosity; Your Best First Line of Defence

Curiosity is not just a nice-to-have trait; it is one of the most overlooked yet effective cyber defence tools.

When people are trained to pause and question what they see, they are more likely to detect a red flag before it becomes a full-blown crisis. Cyber criminals are masters of disguise; they **manipulate trust, exploit routine, and rely on people following instructions without thinking twice.**

Encouraging people to engage their **critical thinking muscles**, to be healthily sceptical, and to question the unexpected, gives your organisation a fighting chance. Studies have shown that when individuals are **more inquisitive** and alert to irregularities, the success rate of **phishing attacks** drops considerably[3].

That quick moment of hesitation before clicking — asking *"Does this seem right?"* — can be the difference between safety and compromise.
Clicking a dodgy link because you were distracted by free doughnuts in the kitchen is relatable. But it's also avoidable, with a bit of **training** and a whole lot of **curiosity**.

Leaders can:

- Normalise asking questions, even the obvious ones
- Publicly praise curiosity and caution
- Share stories where asking the right question stopped a mistake in its tracks

Top tip: Embed curiosity into team rituals.

Embed curiosity into team rituals. Start meetings with a "What looks odd this week?" round. It sharpens instincts and keeps everyone on their toes.

Relevant learning sources in our Learning Library:

- **Unleashing Your Creativity:** Encourages thinking beyond the obvious
- **Fostering Innovation:** Builds confidence to explore and question
- **Growth Mindset:** Develop the right attitude to improve reception to new ideas and concepts
- **Learning Culture:** Create a proactive and transparent workplace environment

Learning highlights:

- **Curious teams** are better at detecting and reporting threats
- A culture of curiosity builds **a more attentive and engaged workforce**
- **Critical thinking** trumps blind compliance in cyber safety

Skill Two: Communication That Connects and Protects

If curiosity is the spark, communication is the fuel...

Poor communication is behind many workplace disasters, including cyber ones; studies have shown that unclear messaging, information silos, and misaligned communication can **directly contribute to cyber incidents**[4].

When instructions are vague or filled with jargon, people either guess or freeze. Neither is ideal when you are under attack. **Effective communication**, especially in high-stakes moments, **reduces uncertainty** and empowers quick, **accurate responses.**

Here's what leaders can do:

- Speak in plain English, especially about complex IT issues
- Translate policies into actions that people understand
- Keep messages short, direct, and relevant
- Use humour or analogies to bring dry content to life - Not to toot our own horn too much, but our **Cyber Security Awareness series** does feature five chuckle-inducing videos that turn a cyber breach into a riveting who-dun-it story. Just saying, it's one way to make essential content stick.

Top Tip:
Create a team glossary of common cyber terms and what they mean.

Learning highlights:

- Clarity helps people act fast and accurately
- Jargon reduces understanding and increases risk[5]
- Strong communication culture boosts team resilience

Skill Three: Emotional Intelligence That Strengthens Cyber Resilience

The emotional impact of cyber attacks is often underestimated. Panic, shame, and fear are all common responses to a slip-up; these emotions often lead to cover-ups rather than collaboration[6].

That is where **emotional intelligence (EQ)** steps in. Managers with high EQ can spot when someone is overwhelmed, create space for honest conversations, and guide their teams through challenges calmly. **It's not just about being nice; it's about being effective.** In a world where routine tasks are being handed to machines, emotional intelligence becomes a clear competitive edge[7]. People don't want a robot for a manager when they're having a rough day or reporting a mistake. **Empathetic leaders** turn problems into progress.

When it comes to cybersecurity, think "people first always", as Sarah Armstrong-Smith, author of **'Understanding the Cyber Attackers Mindset**[8]**,** ' put it.

Leaders who harness the skills of **emotional intelligence** and an understanding of wellbeing help build **psychological safety** within teams that ultimately works as the **best line of defence against cyber attacks.** Let's put it into perspective: Who would you rather tell that you may have caused a cyber breach? A manager who rules with an iron fist, making interns squirm as they step into the office, or a manager who asks for feedback, checks in on how you're doing and is open about their own mistakes? The point is, playing the blame game at any stage of a **cyber attack** is impractical; instead, it's better to use these moments as learning experiences to strengthen a **human-centric defence** for the future.

Relevant learning sources in our **Learning Library:**

- Human Centric Leadership
- Emotional Intelligence
- Leadership Sins

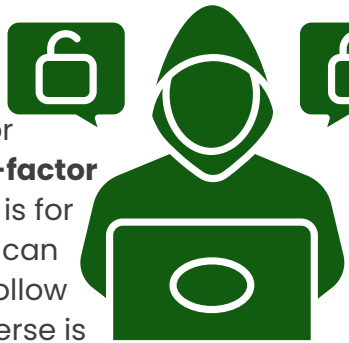
Learning highlights:

- EQ builds trust and openness
- Empathetic responses reduce panic and cover-ups
- Strong EQ supports change management and team cohesion

Skill Four: Role Modelling That Shapes Cyber Culture

Culture eats policy for breakfast. And your cyber culture is only as strong as what your leaders do, not what they say.

People copy what they see. If the boss shrugs off training, uses "password123" or pretends **multi-factor authentication** is for the interns, you can bet others will follow suit. But the reverse is also true. **Leaders** who lead from the front set the tone for everyone else.



Strong cyber role modelling looks like:

- **Asking questions** in front of others to normalise it
- Talking openly about **threats** and **actions** in meetings
- Demonstrating **good digital hygiene** every day

Relevant learning sources in our Learning Library:

- Leadership vs Management: Explores the power of consistent action
- Build a Challenger Network: Shows how openness drives behaviour change
- Psychological safety series

Top Tips:

- **Visibility matters:** Make your good habits visible to teams.
- **Narrate your learning:** Let people know when you have updated a password or spotted a phishing attempt.

Skill Five: Coaching That Makes Cyber Simpler

Coaching is not just for performance reviews. It is one of the most effective ways to help people absorb and retain complex information[9]. Which is handy, because cybersecurity, with all its TLAs (three-letter acronyms) and intimidating interfaces, can quickly go over people's heads.

We forget most of what we learn within a day[10]. Add jargon and pressure into the mix, and retention drops further. Coaching brings learning back down to earth.

Effective leaders will:

- Translate technical updates into relatable risks and actions
- Use real-life examples to spark discussion and build awareness
- Use meetings to simplify cyber protocols, translating the technical into clear actions

Top Tip:

Ask your team to "teach back" what they have learned about a protocol or threat. It boosts memory and shows what they've understood.

Learning highlights:

- Coaching **boosts retention** and **builds confidence**
- Coaching turns awareness into **habit and action**

A Note on AI Proficiency and Cyber Security

AI is not just a buzzword; it is a shapeshifter. From mimicking voices to generating believable phishing emails, it is giving cyber criminals a new set of tools. And they are not shy about using them.

This is why AI proficiency matters. Not in a "become a data scientist by Friday" kind of way, but in understanding how these tools work, how they are used, and when something smells fishy (digitally speaking).

The total value of fraud committed using deepfakes alone has been estimated at up to $4.2 billion, according to Electronic Payments International. Criminals are using AI-generated impersonations to bypass security checks, such as cloned customer voices fooling banks or video avatars of senior executives requesting sensitive information.

It's also worth noting that by uploading data to large AI models or tools, we may unintentionally aid cyber criminals in gathering and analysing private information. Therefore, as AI-driven threats evolve, vigilance becomes everyone's responsibility.

While AI can certainly present risks, it is not all bad. When understood and harnessed effectively, AI can open up a world of benefits in the workplace. It can help by automating tedious tasks, improving decision-making, and even checking the tone and intent of phishing emails. Our AI Anxiety course delves into these realities, helping you overcome fears and embrace AI's potential. We encourage you to explore this course and our wider AI-oriented resources for free to better understand and adapt to this changing environment.

Top Tips to Stay Ahead:

- **Communicate regularly with your IT team:** Keep up to date on the latest AI-driven cyber threats and defence strategies.
- **Stay informed on technological trends:** Follow trusted sources and updates to understand how AI continues to evolve.
- **Share knowledge within your team:** Help everyone stay vigilant by passing on relevant information and best practices.
- **Explore training resources:** Take advantage of courses like our AI Anxiety programme to build confidence and understanding around AI's impact.

Final Thought: Build the Human Firewall

Your tech can only go so far. Firewalls and filters cannot catch everything. **What keeps your organisation safe is your people.**

And not just any people — informed, curious, communicative, emotionally intelligent, and well-coached people.

Cybersecurity is a human issue. And humans, when equipped with the **right skills and support**, are the most effective firewall you can build.

To learn more about strengthening cyber leadership and empowering your teams to tackle evolving threats, feel free to **get in touch**. We'd be glad to share insights and support your journey towards a stronger security culture.

Contact Us

Need help getting started?

Explore our course collections and see how we intergrate storytelling in each one!

AI Anxiety

Mental Health & Wellbeing

Human-Centric Leadership

Diversity & Inclusion

Management Essentials: Motivating your Team

Embracing a Learning Culture

SCAN ME

Get in touch *to discuss your needs and explore the full library!*