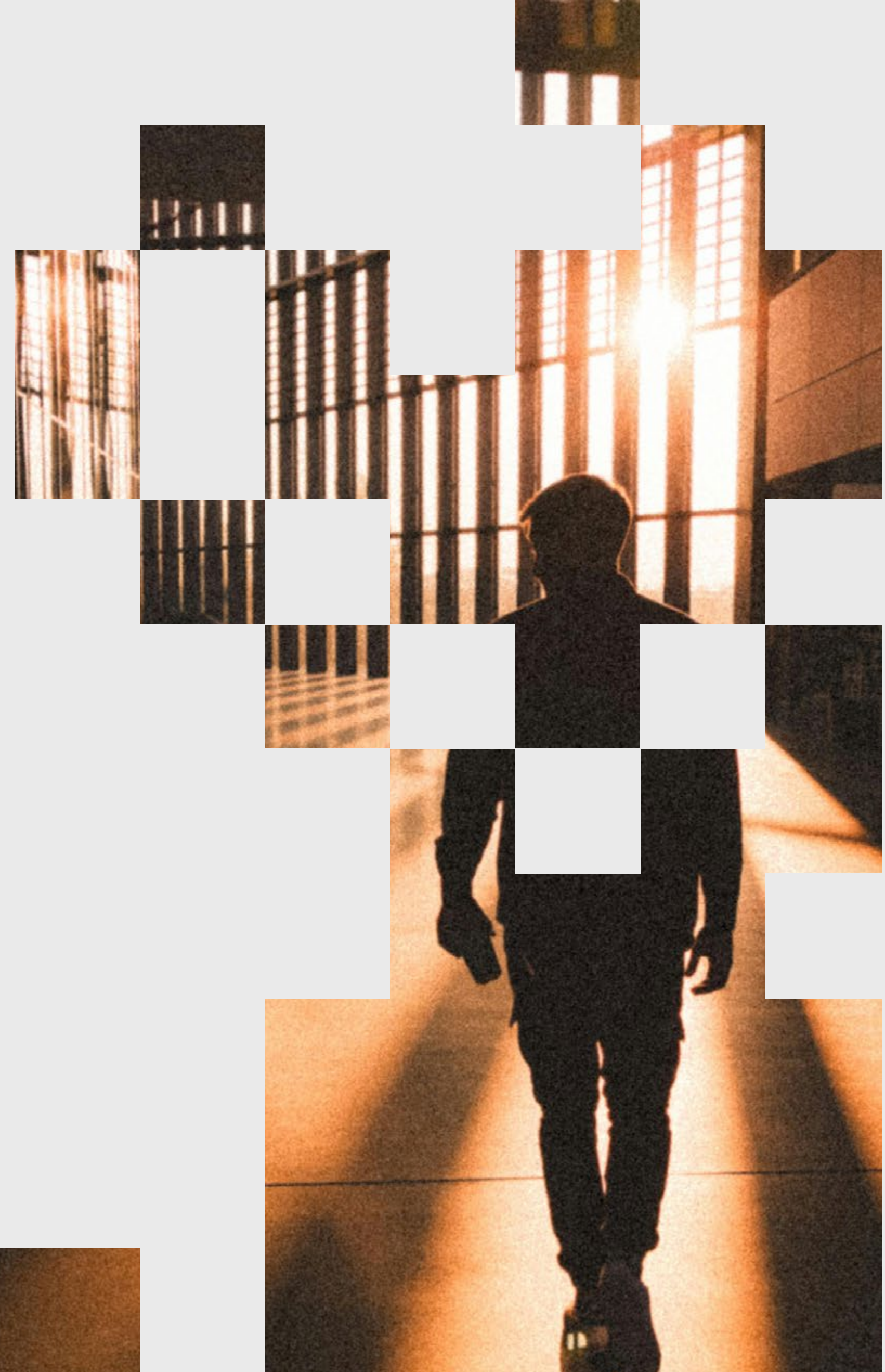


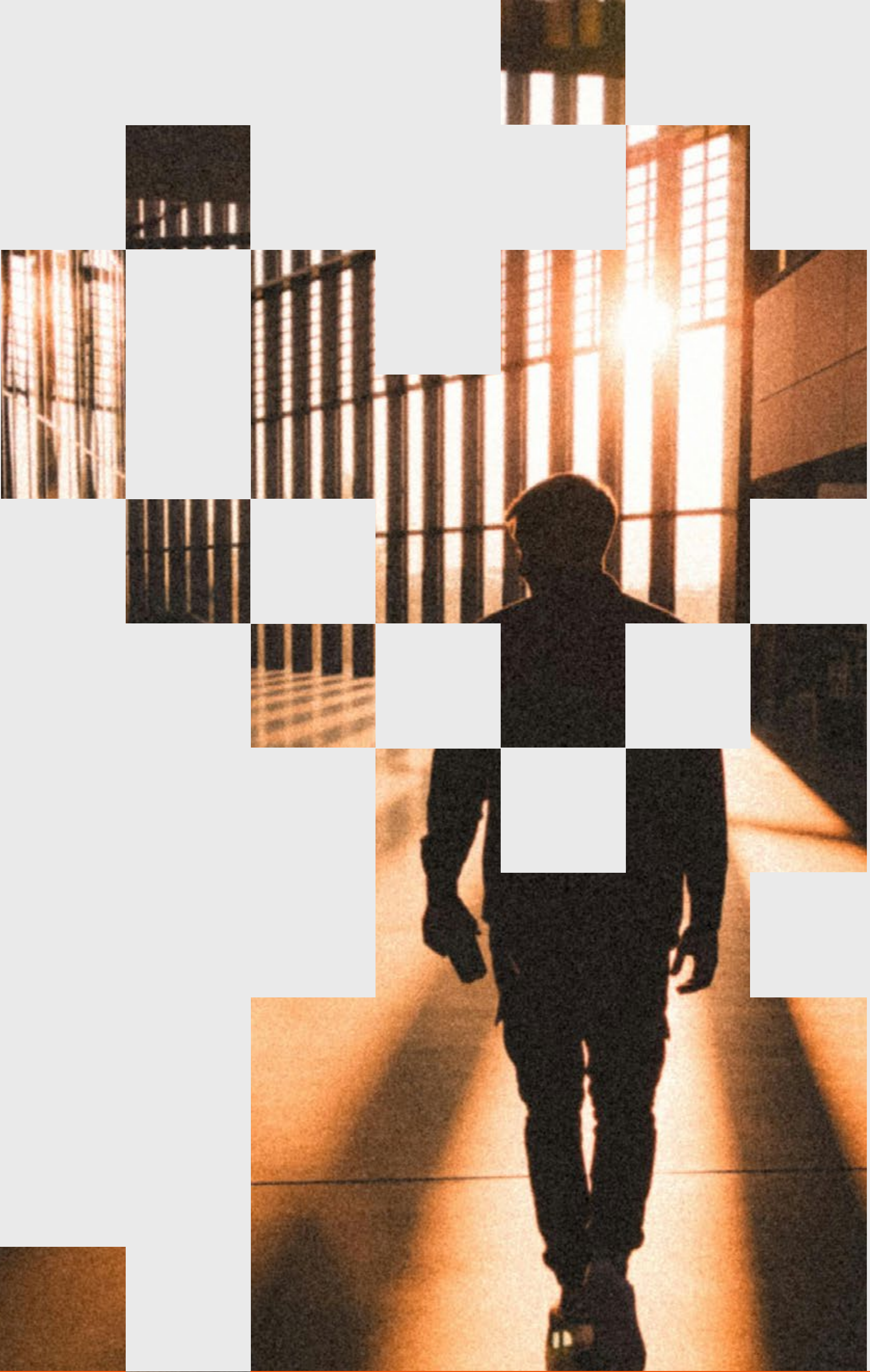
CYBIT

THE 7 STEPS OF HOW CYBER INCIDENTS ESCALATE AND A GUIDE TO PREVENTION.



CONTENTS:

CASE STUDY	3
EXECUTIVE SUMMARY	4-6
FOREWORD	7
HOW TO USE THIS GUIDE	8-9
WHY “CHAIN THINKING” WORKS	10-11
THE UK REALITY (SMB & MID-MARKET)	12-14
LEGAL & REGULATORY REALITY	15
INSURANCE & INSURABILITY	16
THE CYBER 7 STEPS	17-23
SUMMARY	24
NOTES TO EDITORS	25
ABOUT CYBIT	26



CASE STUDY: FROM PHISHING EMAIL TO OPERATIONAL SHUTDOWN

A mid-sized UK organisation experienced a cyber incident that began with a single phishing email.

An employee received a convincing message appearing to come from a trusted supplier. After clicking a link and entering credentials, the attacker gained access to their account.

Over the following days, the attacker:

- Accessed internal systems using valid credentials
- Moved laterally across the network
- Established persistence through additional accounts

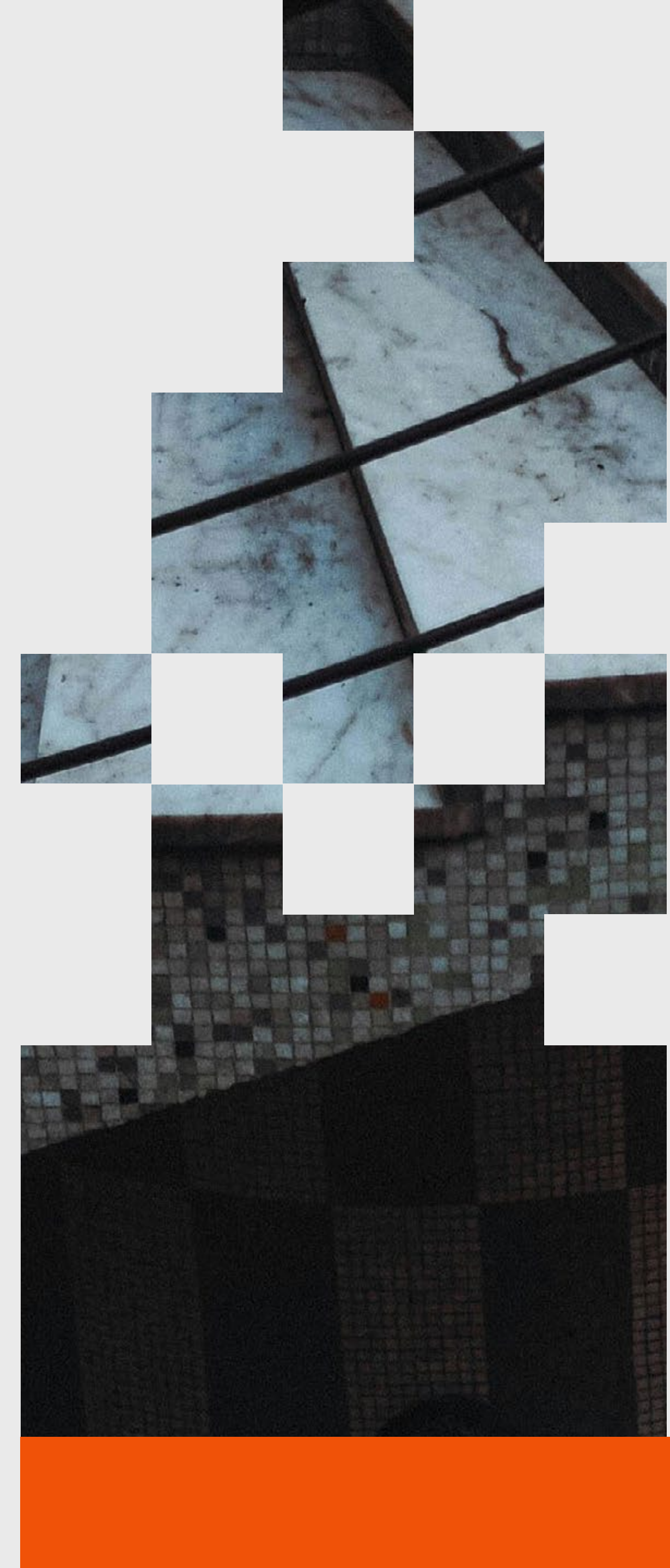
By the time unusual activity was detected, ransomware had been deployed – impacting critical systems and halting operations for several days.

Where the chain could have been broken:

- **Delivery:** stronger email filtering and user awareness
- **Exploitation:** MFA preventing credential misuse
- **Installation:** faster detection of new account and persistence

Outcome:

Operational disruption, recovery costs, and reputational impact – all originating from a single point of entry.



EXECUTIVE SUMMARY:

Cyber risk is no longer a technical issue – it is a business continuity, regulatory, and insurability risk.

Across the UK, organisations face sustained and increasingly targeted cyber activity. For many, a single incident can lead to operational disruption, regulatory exposure, unplanned cost, and lasting reputational damage.

Recent UK government data shows 43% of businesses experienced a cyber security breach or attack in the past 12 months – around 612,000 organisations. Among mid-sized companies, this rises to 67%, highlighting the pressure on those without extensive in-house security resources.

The pattern is consistent. Phishing remains the most common entry point, involved in 85% of incidents. What starts as a single moment – a convincing email or misplaced click – can quickly escalate.

43%

BUSINESSES EXPERIENCED
A CYBER SECURITY
BREACH OR ATTACK

67%

RISES TO THIS AMONGST
MID-SIZED COMPANIES

85%

OF INCIDENTS START AT
PHISHING ENTRY POINTS

EXECUTIVE SUMMARY:

BECAUSE ATTACKS ARE NOT A SINGLE EVENT. THEY ARE A SEQUENCE.

From reconnaissance through to data loss or disruption, attackers build access, escalate privileges, and increase control. As momentum builds, the cost, complexity, and regulatory implications of response rise sharply.

For organisations handling personal data, incidents may trigger legal obligations – including breach assessment and potential notification to regulators within defined timeframes. In parallel, insurers are placing increasing emphasis on demonstrable security controls, with gaps impacting coverage terms, premiums, and even the ability to obtain cyber insurance.

This creates a new reality for business leaders: cyber resilience is no longer optional or isolated within IT – it is a board-level responsibility tied directly to risk, compliance, and commercial viability.

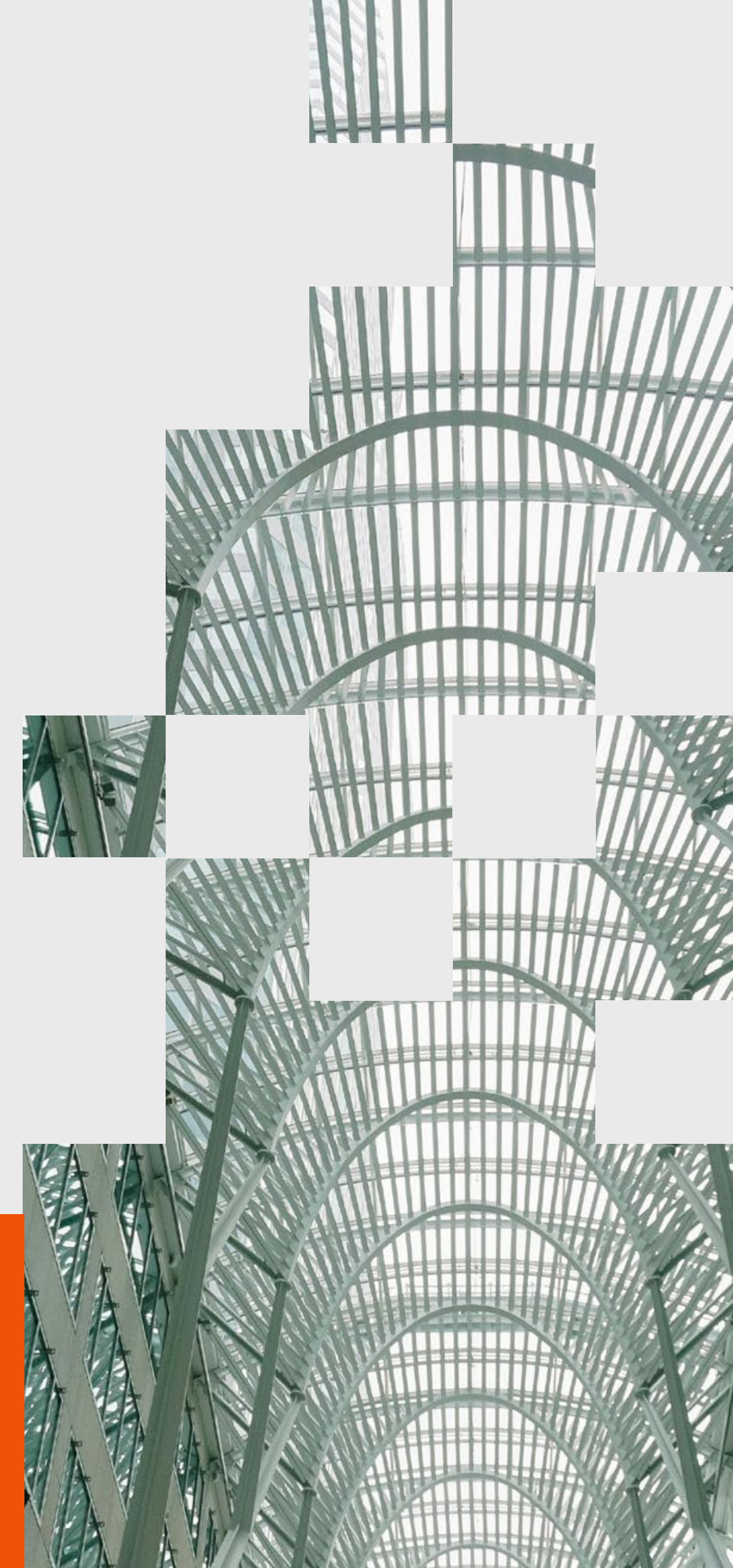
This is where many organisations struggle. Security investments are often made in isolation – tools, controls, policies – without a clear view of how they work together to stop an attack progressing.

This guide takes a different approach.

Using the Cyber**7 STEPS** as a practical framework, it breaks down the seven stages of a modern attack and shows where organisations can intervene to disrupt it. The goal is simple: identify where you are most exposed, and where focused action will reduce risk fastest.

For each stage, you will find:

- What's happening
- Why it matters
- What good looks like
- Common gaps
- A short self-assessment checklist



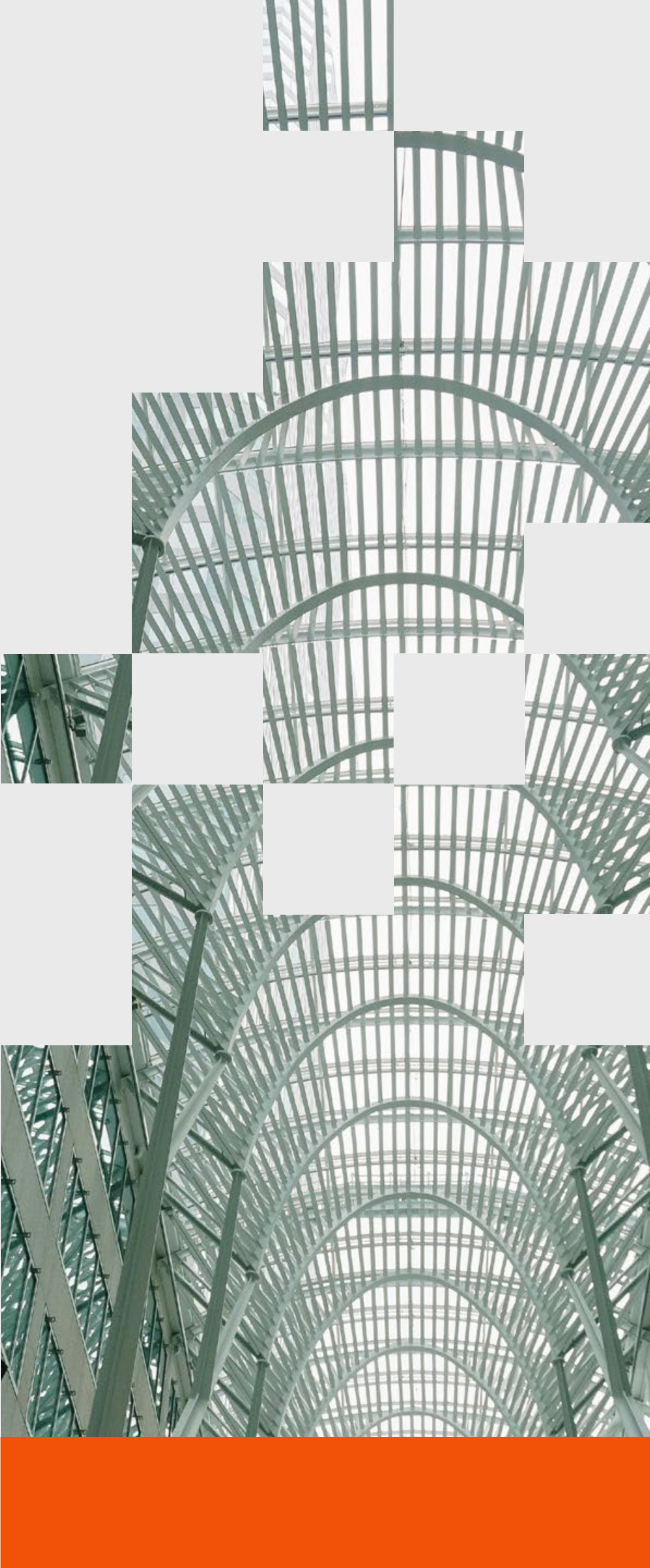
EXECUTIVE SUMMARY:

Together, these stages provide a structured way to move from reactive security to proactive risk reduction—breaking the chain before impact occurs.

For companies that want an independent view, Cybit offers a Cyber Assessment to identify “chain break” opportunities across people, process, and technology.

Ultimately, cyber risk is not just about systems – it is about business consequence. The difference between a contained incident and a major disruption can determine regulatory exposure, insurance viability, and long-term brand trust.

References:
Cyber security breaches survey 2025 | Cyber Security Survey
Cyber Security Statistics | IBM Report



FOREWORD:

Most security leaders we speak to share the same frustration: you can do a lot of things “right” and still feel like you’re one incident away from catastrophe.

That’s because modern cyber attacks are not a single event. They are a sequence – reconnaissance, delivery, exploitation, persistence – each step building momentum. As that momentum grows, options narrow and business impact escalates.

The good news is that this same sequence gives us a structure to defend against. By understanding how attacks progress, organisations can design controls to disrupt them – and identify where they are most exposed.

In the UK, the data is clear: breaches are common, and phishing remains the primary entry point. But this isn’t about fear – it’s about preparation and prioritisation.

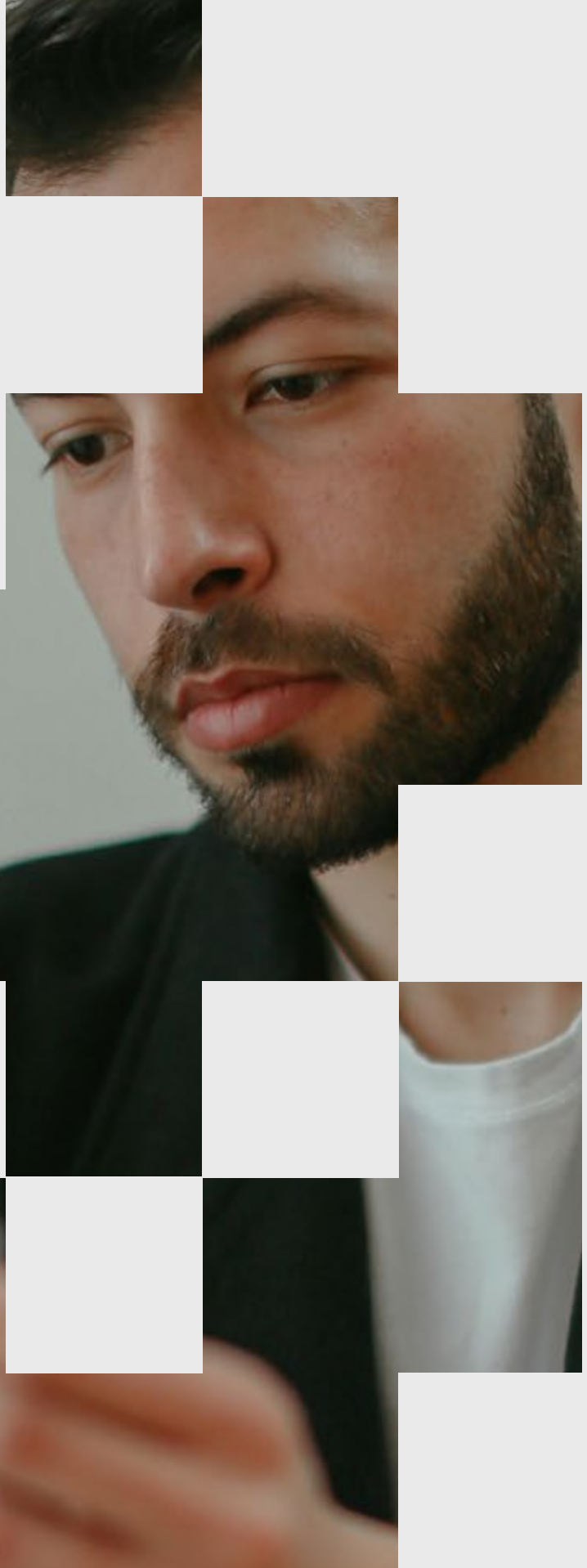
This guide is intentionally practical. It is designed for leaders who need to communicate risk in business terms, prioritise investment, and build confidence that – if an attacker gets in – you can stop or contain them quickly.

If this guide helps you strengthen just one weak link, it has done its job.

BEN LARGE LEAD SECURITY ARCHITECT



YOU CAN DO A LOT OF THINGS “RIGHT” AND STILL FEEL LIKE YOU’RE ONE INCIDENT AWAY FROM CATASTROPHE.



HOW TO USE THIS GUIDE:

Cyber security guidance often falls into two extremes: too technical to act on, or too high-level to be useful. This guide aims to sit in the middle – practical, structured, and focused on what reduces risk.

It is built on a simple idea: **attacks follow a sequence**. By understanding that sequence, you can identify where you are most exposed and take targeted action.

Who this guide is for:

Leaders with accountability for cyber risk, including:

- C-Suite leaders, MDs and CEOs
- CIOs, CISOs, and Security Leads
- IT Directors and Heads of Infrastructure
- Operational and business leaders responsible for resilience and continuity

What you'll get

For each stage of the Cyber **7 STEPS**:

- What's happening
- Why it matters
- What good looks like
- Common gaps
- Signals to watch
- Rapid wins
- Self-assessment checklist

HOW TO USE THIS GUIDE:

How to approach it:

YOU DON'T NEED TO READ THIS COVER TO COVER. INSTEAD:

1.

Start with a high-level review

Familiarise yourself with the seven stages and how attacks progress

2.

Identify areas of uncertainty or weakness

Use the checklists to highlight where visibility, control, or confidence is lacking

3.

Prioritise where action will have the greatest impact

Focus on the stages where a break in the chain would significantly reduce risk

4.

Build a focused action plan

Use the “rapid wins” and control guidance to define practical next steps

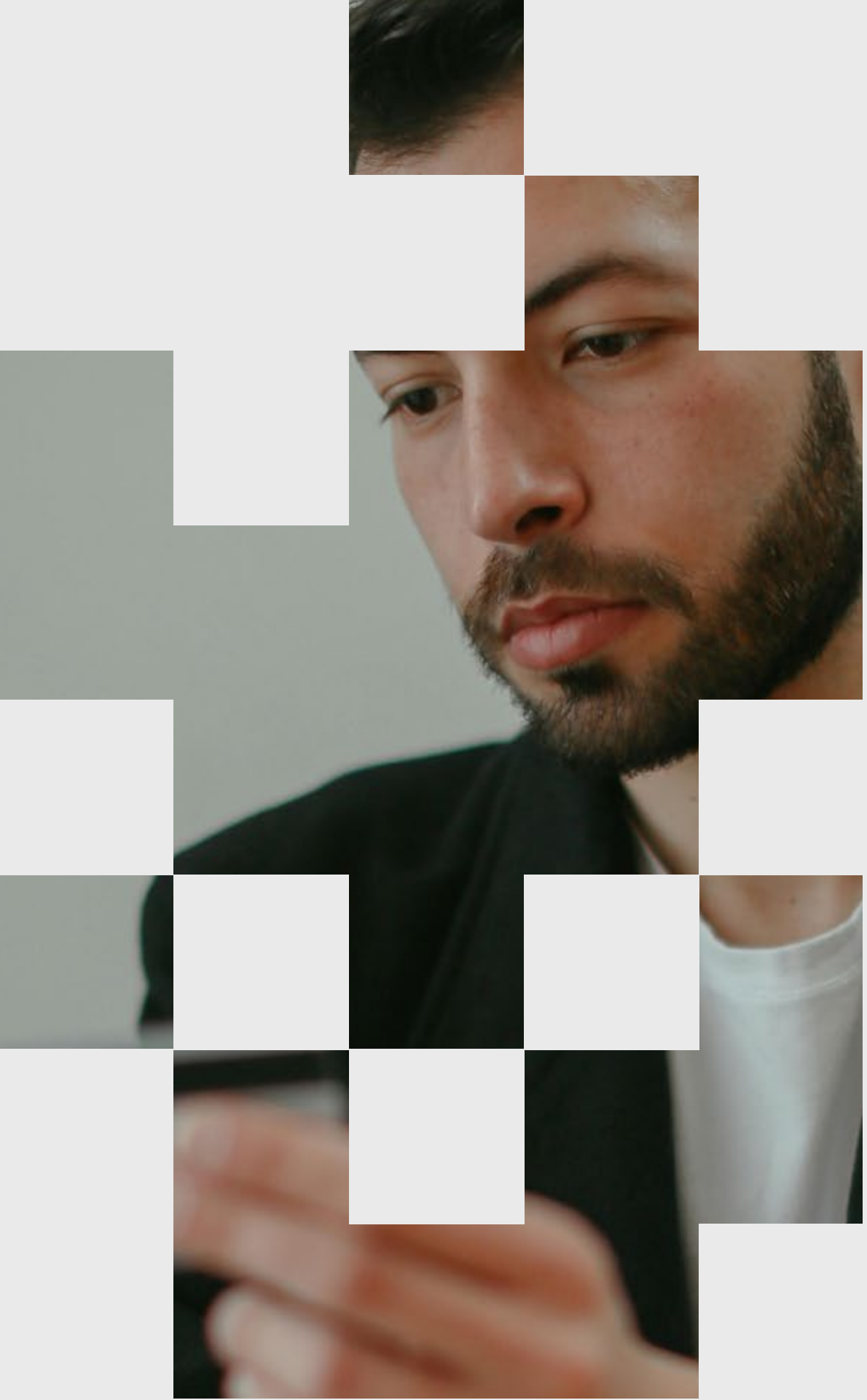
From insight to action:

For many businesses, the challenge is not awareness – it is prioritisation.

Understanding where you are exposed is one thing. Knowing what to fix first, and how those changes work together, is another.

This is where an external perspective can help.

Cybit’s Cyber Assessment provides a structured, independent view of your organisation’s exposure across all seven stages of the attack chain – highlighting the most effective opportunities to “break the chain” across people, process, and technology.



WHY “CHAIN THINKING” WORKS

Most businesses don’t lack security tools – they lack clarity on how those tools work together.

Security is often managed in silos, while attackers follow a sequence. Each step builds on the last – access, escalation, persistence, control – until disruption occurs.

RISK IS NOT A SINGLE FAILURE. IT IS A CHAIN OF SMALL GAPS.

Attacks progress in steps. Your controls should too.

“Chain thinking” shifts the focus from isolated controls to coordinated defence.

Instead of asking: “Do we have the right tools”

It asks: “At which stage would we actually stop an attacker?”

This is a critical difference.

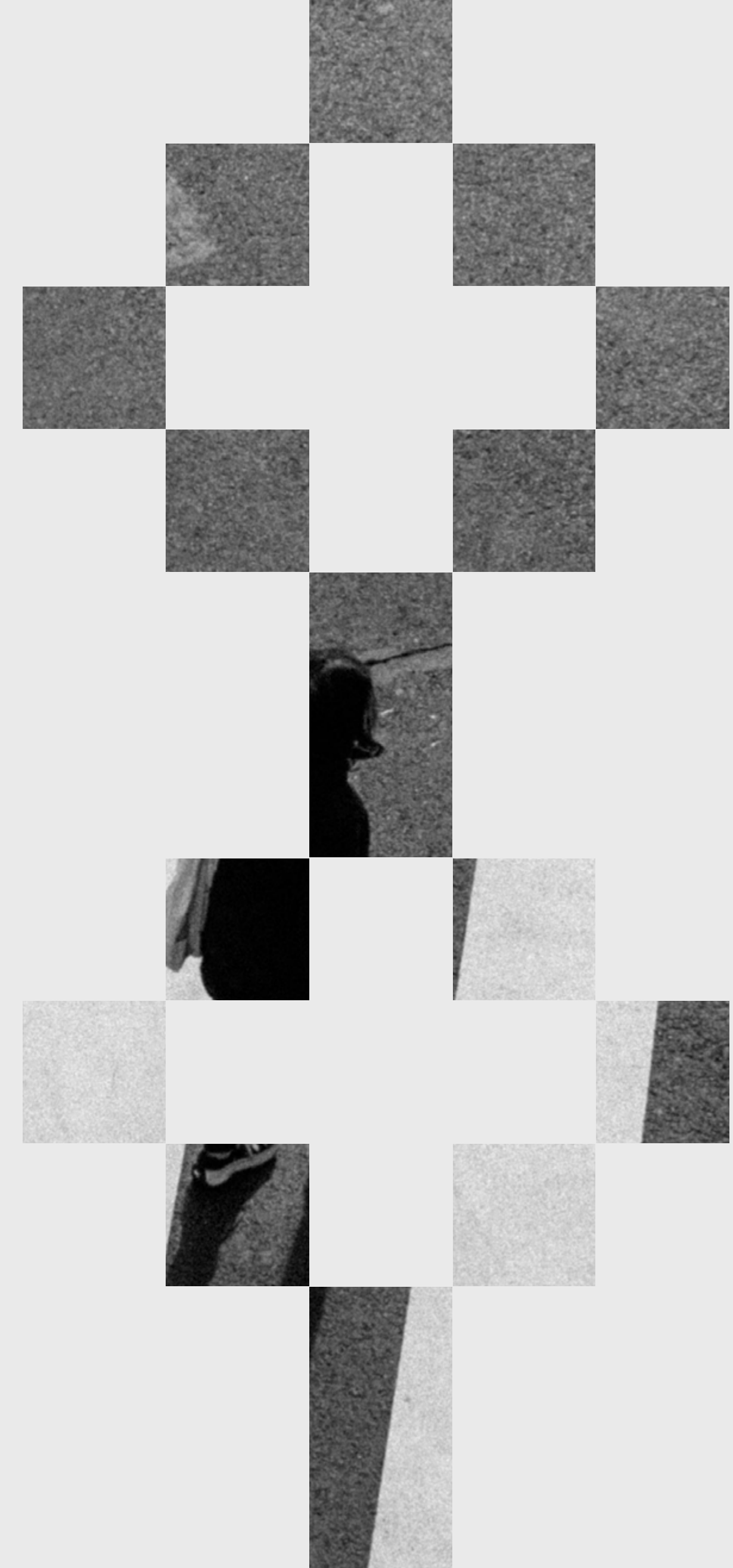
A well-placed control at the right stage can significantly reduce risk – even in constrained environments.

Breaking the chain early changes everything

The earlier an attack is disrupted, the lower the impact.

- Stopping a phishing email from reaching a user is low cost and low disruption
- Detecting and containing a compromised account is more complex
- Recovering from ransomware or large-scale data loss is costly, time-consuming, and highly visible for the business

Yet many organisations are strongest at response – and weakest at prevention.

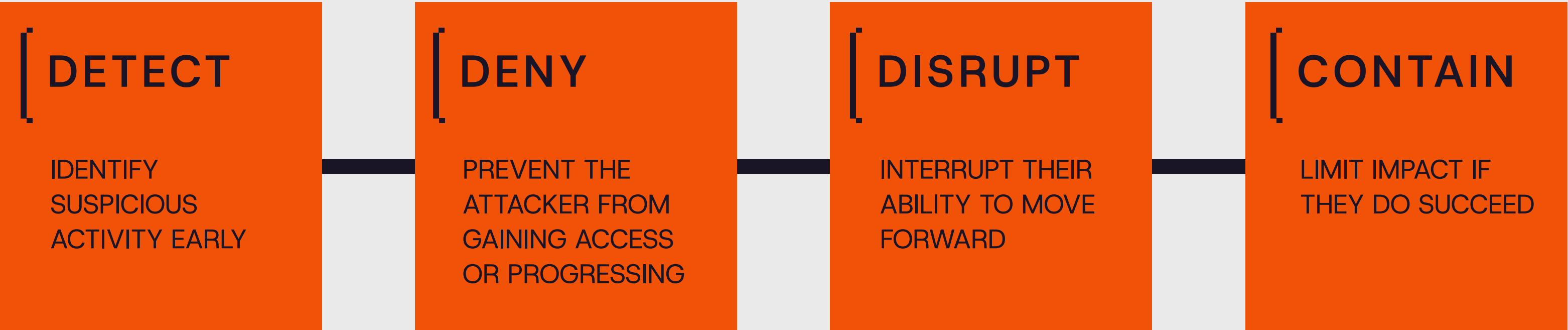


WHY “CHAIN THINKING” WORKS

A simple defence lens:

At each stage of the chain, effective defence comes down to four outcomes:

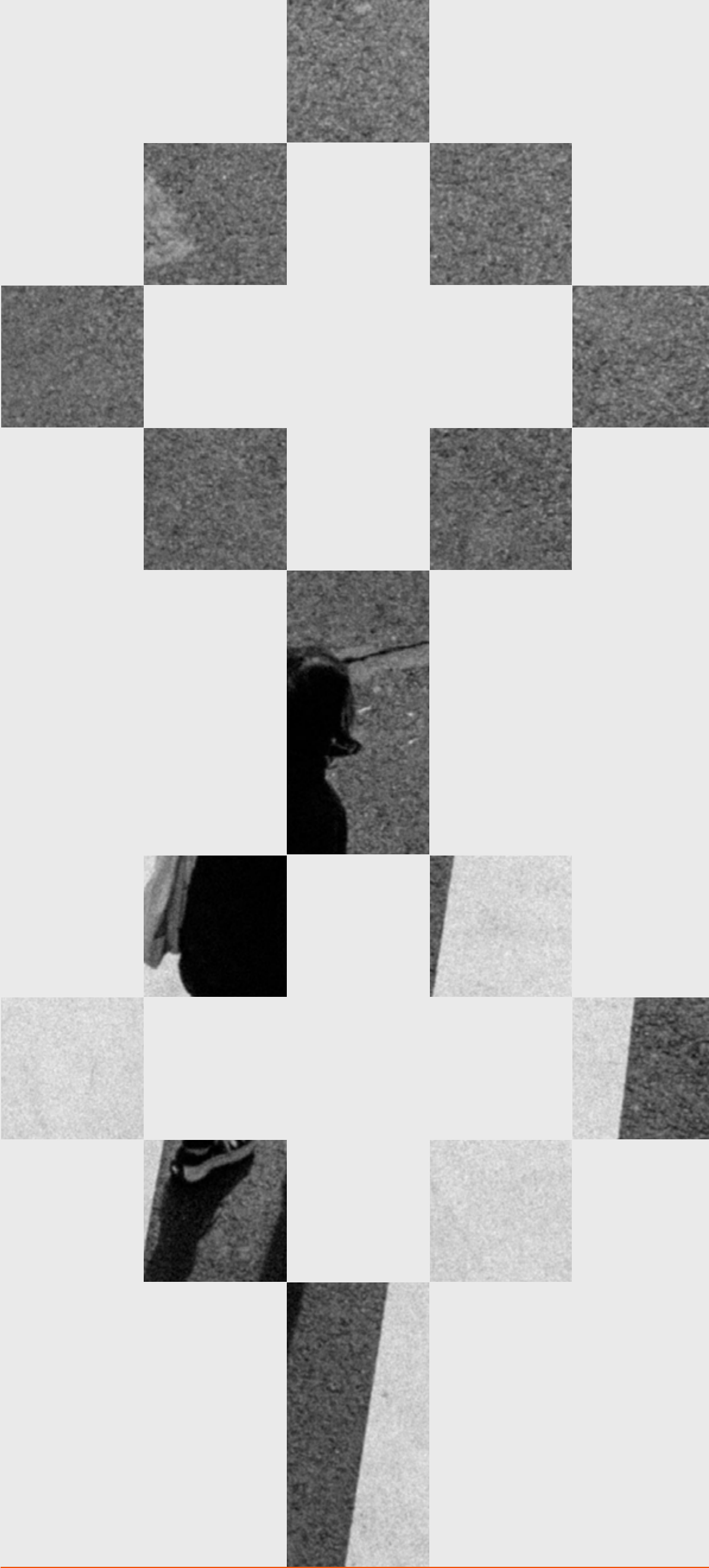
Understanding where you can do this – and where you cannot – gives a clear view of risk.



A widely adopted model

The Cyber **7 STEPS** is a framework to describe how attacks unfold. While every company is different, the underlying pattern is consistent enough to provide a useful structure for both assessment and improvement.

This guide uses it to help you identify gaps, prioritise action, and align security to real-world attack behaviour.



THE UK REALITY (SMB & MID-MARKET)

The UK reality (SMB & Mid-Market)
Cyber attacks are not a future risk – they are a current and persistent reality.



43% of businesses experienced a breach in the past year, rising to 67% for mid-sized organisations. As businesses grow, so does the exposure.

This reflects increased digital footprint, complex supply chains, and a broader attack surface.

A consistent pattern: phishing

Despite advances in security technology, most attacks still begin in a familiar way: phishing, which is involved in 85% of reported breaches.

Attackers often rely on simple tactics:

- Busy employees
- Inconsistent awareness
- Gaps in email and identity controls

A single email can lead to credential theft and wider system access.

From minor incident to major disruption

One of the most common misconceptions is that cyber incidents are isolated or contained events.



THE UK REALITY (SMB & MID-MARKET)

The impact often escalates.

An initial compromise – such as a stolen password – may go unnoticed. Over time, attackers can:

- Expand across systems
- Maintain long-term access without being detected
- Identify high-value data or critical services
- Position themselves for maximum impact

By the time action is taken, the situation is no longer a minor security issue, it is a business disruption event.

The cost of a breach –
and the cost of delay

The financial impact of cyber incidents varies widely, but the direction of travel is clear: costs increase rapidly as attacks progress.

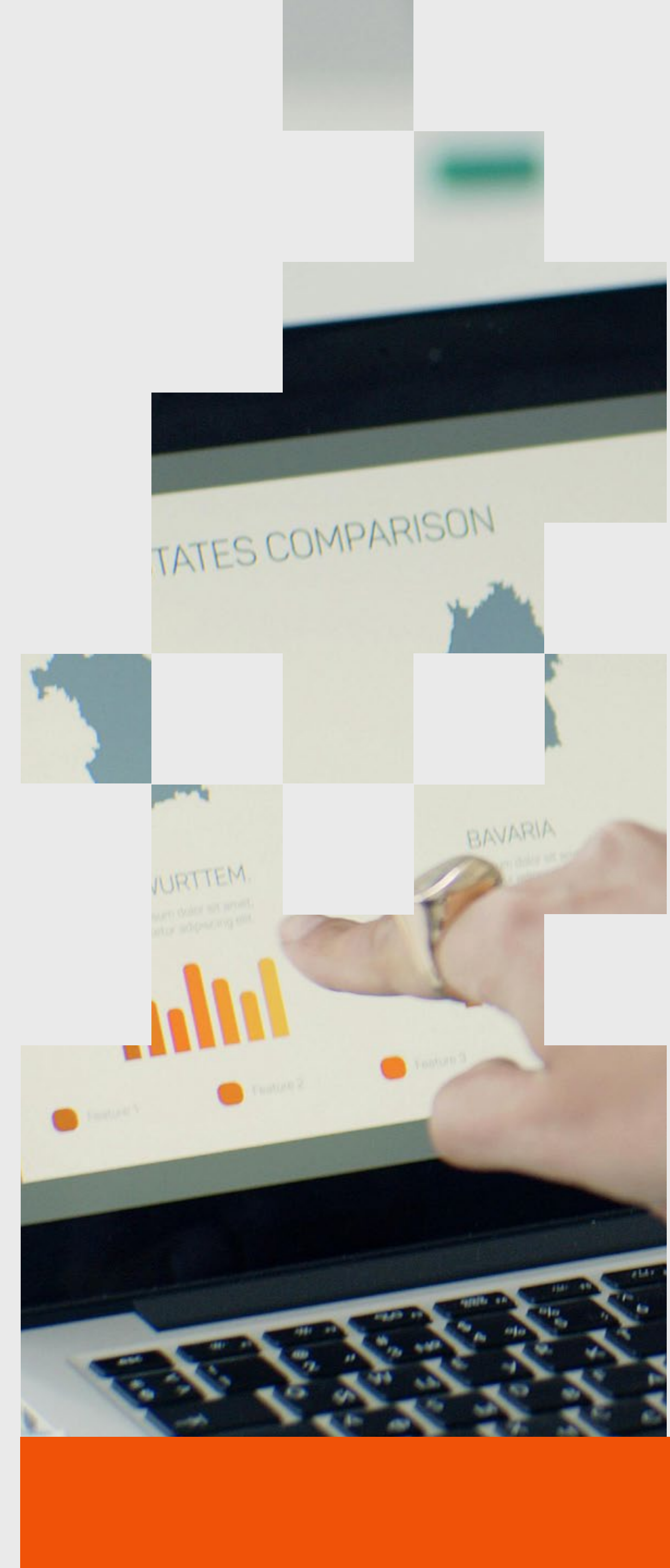
- Severe incidents reach millions
- Longer detection times increase impact
- Strong detection reduces cost and recovery time

In other words, the difference between a contained incident and a major breach is often timing.

Why SMB and mid-market organisations are targeted

It is a common assumption that attackers focus primarily on large enterprises. But SMB and mid-market companies are frequently targeted – and often more vulnerable.

This is not because they are less important, but because they present a different kind of opportunity:



THE UK REALITY (SMB & MID-MARKET)

- **Limited in-house security resource**
Smaller or stretched teams managing a wide range of responsibilities
- **Tooling without full integration**
Security controls in place, but not always aligned or optimised
- **Identity and access complexity**
Growing user bases, third-party access, and inconsistent privilege management
- **Patching and visibility gaps**
Limited capacity to maintain full visibility across all assets and vulnerabilities
- **Supply chain exposure**
Increasingly targeted as a route into larger partner ecosystems

Attackers understand these dynamics. They are not looking for the hardest target – just the one where a sequence of small weaknesses can be combined into a successful attack.

The implication: risk is cumulative

Risk does not come from a single major failure. It builds over time:

- An exposed system that is not fully tracked
- A user with more access than they need
- A delayed patch
- A missed alert

Individually, these issues may seem manageable. Together, they create conditions for an attack to succeed. This is why a structured approach – one that looks at how attacks unfold – is critical.



LEGAL & REGULATORY REALITY

Cyber incidents are not just technical events – they can trigger legal, regulatory, and commercial consequences.

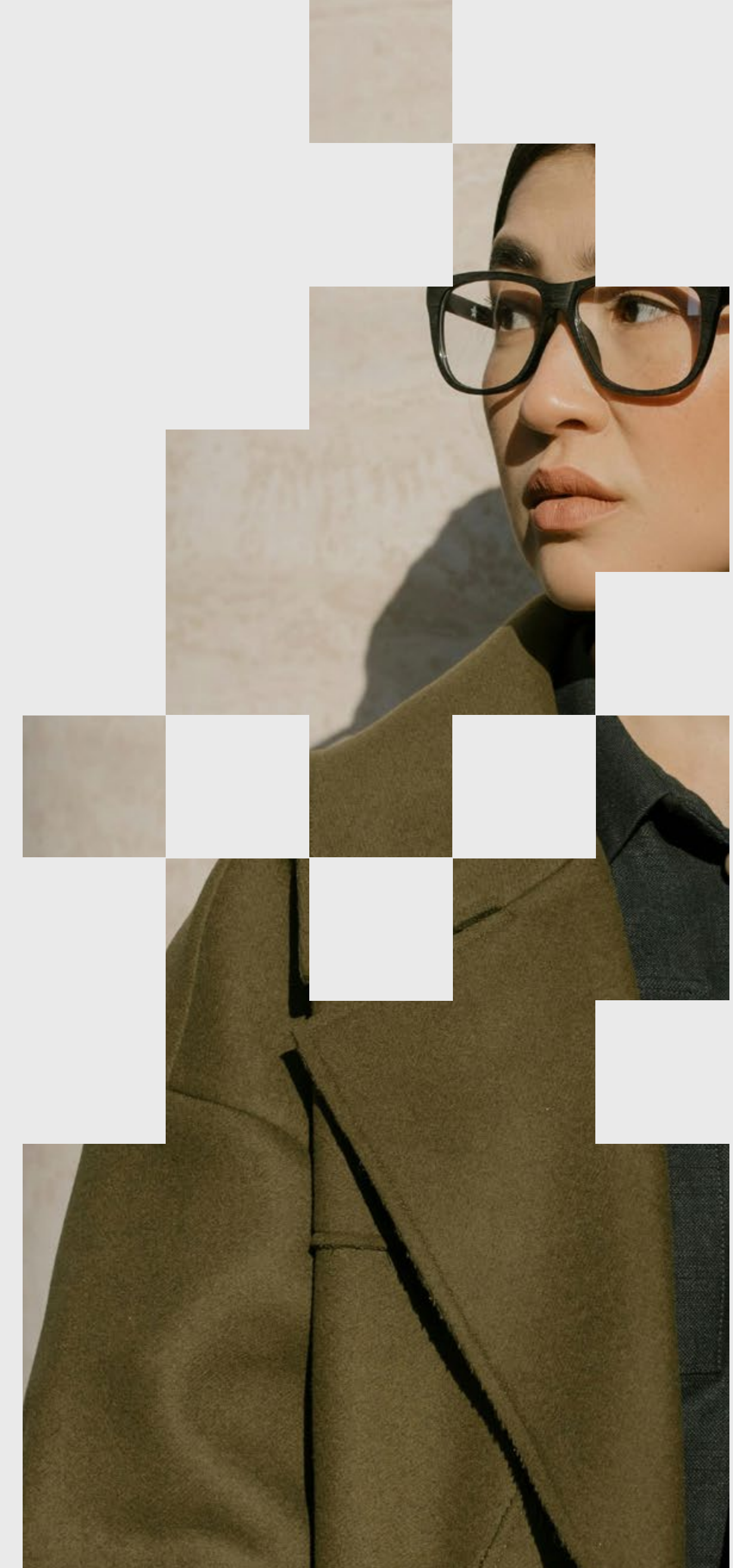
For many UK organisations, a breach involving personal data may require assessment and, where risk is identified, notification to the Information Commissioner's Office (ICO) within 72 hours, as well as communication to affected individuals in serious cases.

Certain sectors face additional obligations. Operators of essential services and digital providers must meet resilience and incident reporting requirements under NIS regulations. Financial services organisations – and those supplying into them – are subject to operational resilience expectations in the UK, and, in the EU, the Digital Operational Resilience Act (DORA), which introduces formal requirements around ICT risk, testing, and third-party oversight.

Even where formal regulation is limited, expectations on leadership are increasing. Boards are expected to understand cyber risk, oversee controls, and ensure incident response readiness – including supply chain risk.

Alongside this, cyber resilience is becoming a commercial requirement. Insurers are placing greater emphasis on demonstrable controls, with gaps affecting premiums, coverage, and insurability. Customers and partners are also increasing scrutiny through contractual and supply chain requirements.

The implication is clear: cyber risk now carries legal, financial, and commercial consequences. The ability to prevent, detect, and respond to incidents – and to demonstrate that capability – is critical.



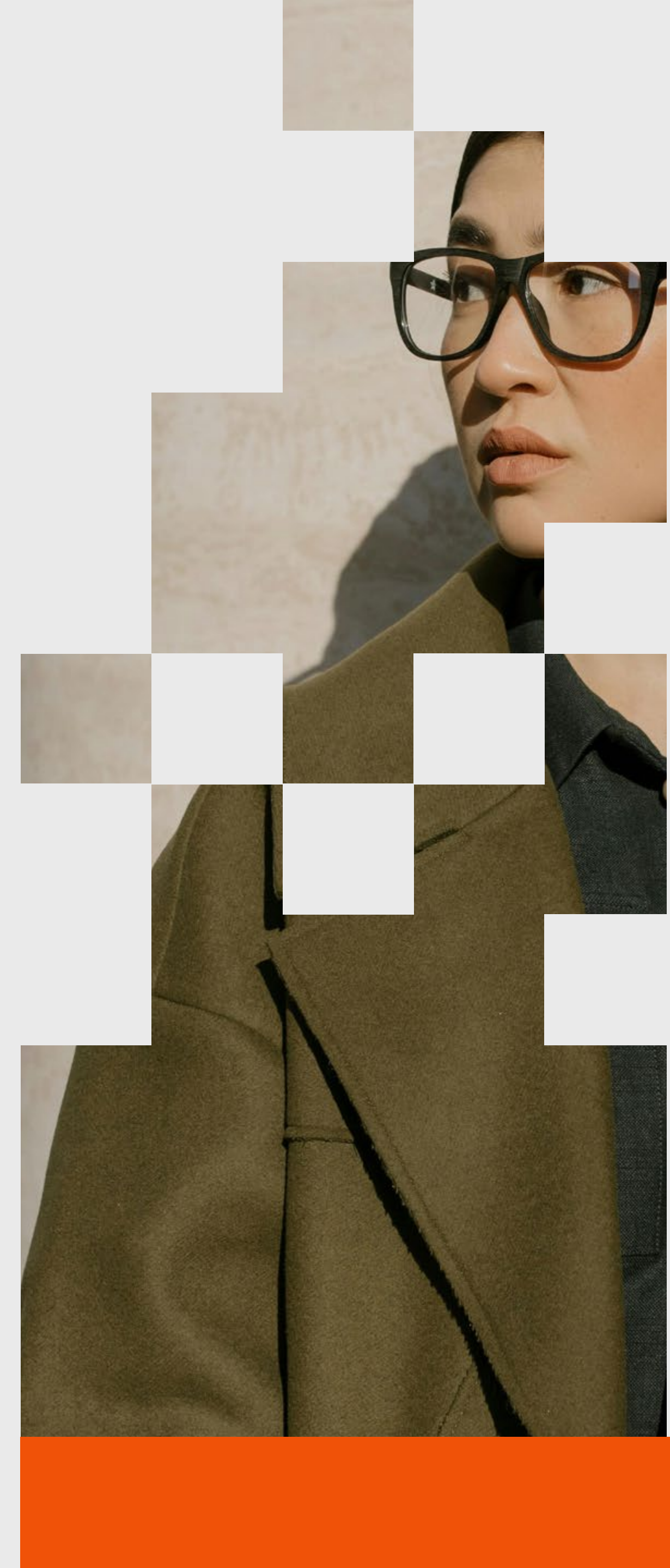
INSURANCE & INSURABILITY: A SHIFTING COMMERCIAL REALITY

Cyber insurance is increasingly tied to demonstrable security controls, not just risk transfer. Market commentary from major brokers indicates that underwriting decisions are now influenced by governance maturity, incident readiness, and technical control baselines.

This means cyber insurance is no longer a passive safety net. It is becoming a conditional outcome of cyber maturity.

Organisations with weaker controls may face higher premiums, reduced coverage, stricter terms, or in some cases challenges obtaining cover at all. Conversely, those able to demonstrate structured, tested controls and incident readiness are better positioned in a tightening insurance market.

In practice, insurance is becoming a reflection of cyber resilience – not a substitute for it.



THE CYBER 7 STEPS

To understand how this risk plays out in practice, we need to look at how attacks unfold.

Stage 1 – Reconnaissance (pre-attack)



What happens

Attackers look for weak points before they strike. They scan public sources – LinkedIn, company websites, and leaked credentials – to find vulnerable people, systems, or partners. Their goal: to get a foot in the door using information that’s already exposed.

Recon is the “lowest-hanging fruit” stage. Users overshare online, legacy systems exist, and suppliers can introduce gaps. While it doesn’t cause direct damage, it sets up what comes next.

What good looks like:

- Know all your internet-facing assets
- Monitor publicly available information and leaked credentials
- Ensure attack surface visibility – nothing exposed that shouldn’t be

Signals to watch

- Limited signals at this stage
- Watch for unusual login attempts or repeated probes

Rapid wins (30–60 days):

- Enforce strong and regularly changed passwords and multi-factor authentication (MFA)
- Unique passwords across each account and stored in a password vault
- Employees awareness: what can’t be shared publicly
- Standardise IT configurations to avoid accidental exposure

Self-check checklist:

- “Do we know all our internet-facing assets?”
- “Are credentials unique and MFA-enabled?”
- “Are employees and suppliers aware of exposure risks?”
- “Are all Cloud services using MFA for all users and not just admin?”

“DO WE KNOW ALL OUR INTERNET-FACING ASSETS?”

THE CYBER 7 STEPS

Stage 2 – Weaponisation (pre-attack)

2.



What happens

Attackers craft custom payloads using intel from reconnaissance. They exploit human psychology – fake recruiters, malicious documents, or tailored emails – to trick users into giving access.

This is where recon turns into action. A single click or download can open a door, escalate privileges, or spread malware.

What good looks like:

- Prioritise vulnerabilities based on threat intel
- Harden systems, limit or block unsafe file types

Signals to watch

- Suspicious email attachments
- Odd file types

Rapid wins (30–60 days):

- Patch systems and test regularly within 14 days
- Enforce file controls and block unsafe attachments

Self-check checklist:

- “Do we patch based on exposure and exploitability?”
- “Are dangerous file types blocked by policy?”



“ARE DANGEROUS FILE TYPES
BLOCKED BY POLICY?”

THE CYBER 7 STEPS

Stage 3 – Delivery (initial compromise)

3.



What happens

Attackers deliver payloads through phishing, web downloads, USBs, or supplier systems.

This is the point where attackers reach your environment. A successful delivery can lead to credential theft, malware installation, or data access.

What good looks like:

- Assess if personal data is involved and determine risk
- Report to the ICO within 72 hours where required
- Notify affected individuals in high-risk cases
- Maintain incident records
- Strengthen email security, user awareness, and access controls to reduce risk of compromise

Signals to watch

- Spikes in traffic to unusual domains
- Users reporting suspicious emails or downloads

Rapid wins (30–60 days):

- Block unnecessary websites and USB devices
- Encrypt data and enforce internal policies
- Filter spam and unsafe links

Self-check checklist:

- “Are high-risk users protected differently?”
- “Can we recover critical services to a defined RTO?”



“CAN WE RECOVER CRITICAL SERVICES TO A DEFINED RTO?”

THE CYBER 7 STEPS

Stage 4 – Exploitation (gaining access)

4.



What happens

Attackers exploit vulnerabilities – users click links or download malicious files. They may execute code or escalate privileges.

A single exploit can give attackers broader access and a foothold in the organisation.

What good looks like:

- Access to next-gen antivirus or EDR (Endpoint Detection and Response)
 - In-house EDR trained employee to manage this, or outsourced externally
- Hardening systems and reducing attack surface
- Privilege separation and rapid detection enabled

Signals to watch

- Unexpected processes running on devices
- Suspicious credential activity

Rapid wins (30-60 days):

- Lock down devices
- Deny admin rights for general users
- Prevent installation of unwanted applications

Self-check checklist:

- “Do we detect suspicious privilege escalation quickly?”
- “Are devices hardened and monitored?”



“DO WE DETECT SUSPICIOUS PRIVILEGE ESCALATION QUICKLY?”

THE CYBER 7 STEPS

Stage 5 – Installation (persistence & foothold)

5.



What happens

Attackers set up backdoors, scheduled tasks, and new accounts to stay in your environment.

Persistence allows them to move undetected, increasing potential impact over time.

What good looks like:

- EDR persistence detection
- Golden image integrity – a standardised “perfect mold” software setup to default back to in case of attack
- Application allow-listing – only approved apps can run on systems
- Secure admin model

Signals to watch

- Unusual files or software changes
- New scheduled tasks or accounts

Rapid wins (30-60 days):

- Only IT has admin rights
- Enforce Principle of Least Privilege (PoLP) where users, systems and processes operate using the bare minimum access privileges
- Monitor for unusual activity

Self-check checklist:

- “Can we detect new persistence within hours?”
- “Are admin account tightly controlled?”



“ARE ADMIN ACCOUNT TIGHTLY CONTROLLED?”

THE CYBER 7 STEPS

Stage 6 – Command & Control (C2)

6.



What happens

Compromised systems communicate with attackers, allowing remote control.

This is where attackers expand access, move laterally, and potentially exfiltrate data.

What good looks like:

- DNS security and egress control
- Network segmentation and limited ACL's
- Anomaly detection and threat hunting

Signals to watch

- Unusual outbound traffic
- Living-off-the-land (LOTL) tools in action – attackers use these to carry out malicious activities undetected
- Legitimate tools used abnormally

Rapid wins (30-60 days):

- Monitor and block suspicious traffic
- Segment sensitive systems
- Audit for unusual communication patterns

Self-check checklist:

- "Do we inspect unusual outbound traffic and block it?"
- "Are lateral movement paths restricted?"



"DO WE INSPECT UNUSUAL OUTBOUND TRAFFIC AND BLOCK IT?"

THE CYBER 7 STEPS

Stage 7 – Actions on Objectives



What happens

Attackers achieve their goal: data-theft, ransomware, or operational disruption.

This is the stage where business impact becomes unavoidable – lost data, operational downtime, regulatory exposure, and reputational damage.

At this point, organisations may face legal and compliance consequences, including mandatory breach notifications, regulatory scrutiny, and potential financial penalties.

There is also a direct impact on insurability and risk profile. Organisations that cannot demonstrate effective controls, detection, and response capability may face increased premiums, reduced coverage, or difficulty obtaining cyber insurance altogether.

Critically, the brand impact can be long-lasting. Loss of customer trust, partner confidence, and market credibility often extends far beyond the recovery period.

What good looks like:

- Protect sensitive data through encryption, access controls, and data loss prevention (DLP)
- Ensure critical data is appropriately classified, labelled, and restricted

- Maintain a tested and clearly communicated incident response plan
- Ensure response plans align with legal, regulatory, and contractual obligations
- Enable rapid containment and recovery to minimise operational disruption
- Conduct regular incident simulation exercises (e.g. tabletop testing)
- Maintain clear roles and escalation paths for incident response

At this stage, breaches may lead to regulatory action, mandatory notifications, and external investigation. Organisations can also face higher insurance premiums, reduced cover, or difficulty obtaining cyber insurance where controls are inadequate. Beyond compliance and cost, disruption can directly impact revenue, supply chains, and service delivery, while reputational damage often persists long after technical recovery, eroding customer and partner trust.

Rapid wins (30–60 days):

- DLP and encryption for sensitive data
- Prepare incident response plan
- Train staff on reporting anomalies
- Incident response plan and testing

Self-check checklist:

- “Is critical data encrypted?”
- “Can we contain incidents quickly?”
- “Are recovery plans tested?”

SUMMARY:

Cyber attacks succeed not because of a single failure, but because of a sequence of small, unaddressed gaps.

By understanding how attacks progress – and where they can be disrupted – organisations can move from reactive response to proactive risk reduction. This not only reduces the likelihood and impact of an incident, but also strengthens regulatory compliance, insurability, and brand resilience.

In an environment where cyber incidents carry legal, financial, and reputational consequences, the ability to break the chain early is no longer a technical advantage – it is a business imperative.

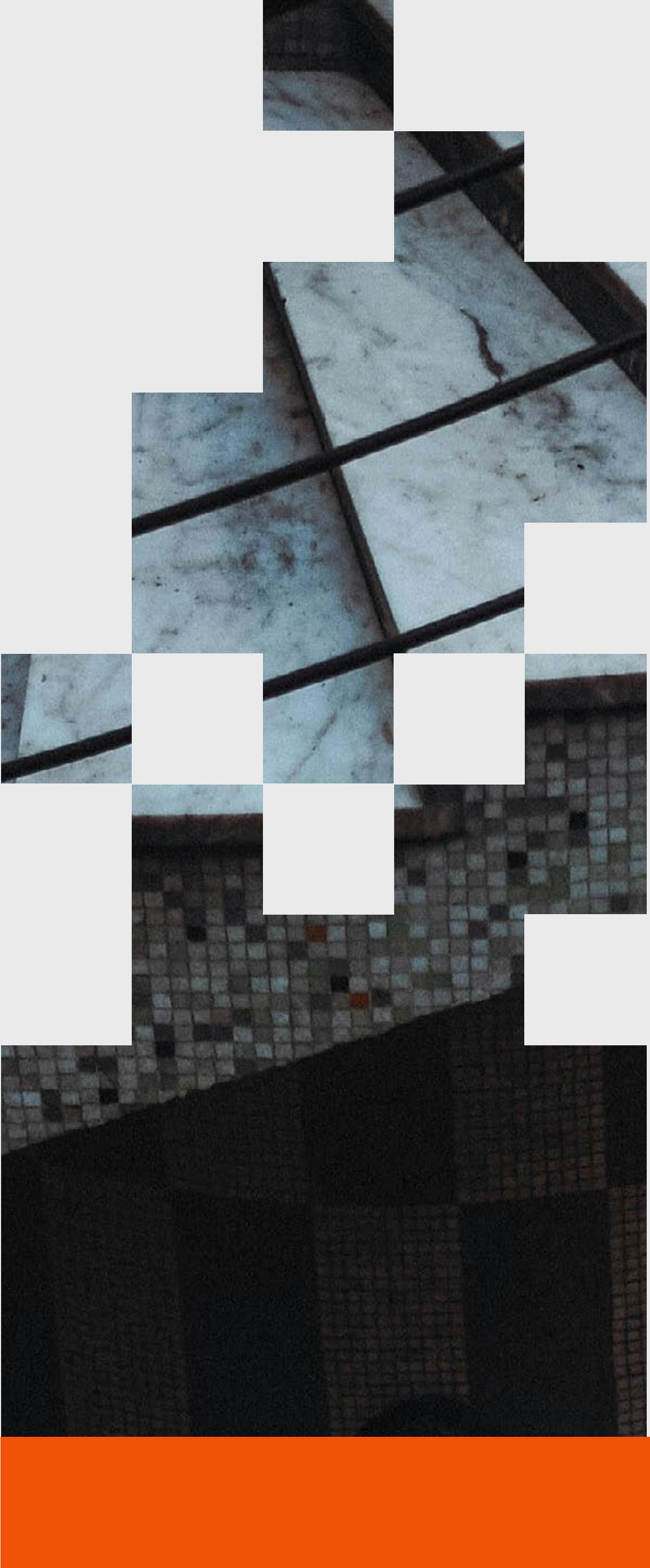
Industry insight:

Ronan Lavelle Co-founder and CEO of Validato
"The Cyber 7 STEPS (and subsequent frameworks, like MITRE ATT&CK) helps cyber defenders better understand adversarial tradecraft so they can prioritise and align their defensive tooling and efforts.

As a business with limited resources and budgets, it is important to spend your time and money on activities that will have the best return on your security investment. Frameworks like the LM Cyber 7 STEPS and MITRE ATT&CK provide the context to be able to make these kind of decisions."

References and supporting sources:

- UK Government: Cyber Security Breaches Survey 2025 (prevalence, phishing, costs, governance trends) — GOV.UK [gov.uk]
- UK Government/NCSC: Cyber Governance Code of Practice — GOV.UK [gov.uk]
- NCSC: Cyber Security Toolkit for Boards — NCSC [ncsc.gov.uk]
- ICO: Personal data breaches: a guide (72-hour reporting, notify individuals, record keeping) — ICO [ico.org.uk]
- EU DORA: applicability date + pillar summary (official circular referencing OJ publication) — MFSA PDF (reputable regulator source) [mfsa.mt]

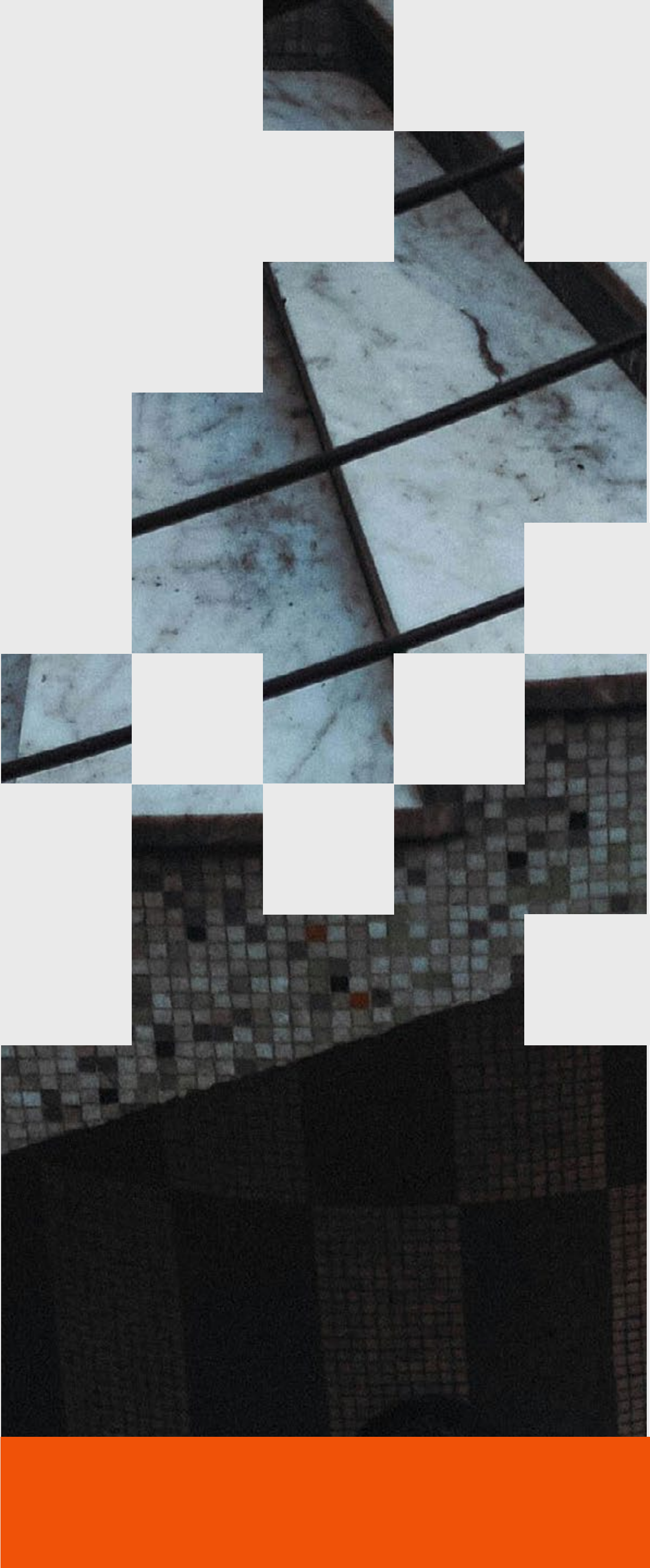


NOTES TO EDITORS – AUTHOR BIOS

Ben Large LEAD SECURITY ARCHITECT

Ben Large joined Cybit in 2025 as Lead Security Architect & vCiso with over 20 years of experience. He provides thought leadership, supporting sales teams, and protecting customers from cyber threats.

Ben excels in creating solutions that drive sales, developing innovative products, and training teams to be vigilant and effective. His passion lies in safeguarding assets, data, and company reputations, as well as mitigating and hunting insider threats. He has worked with FTSE 50 and various sectors, including Government, Finance, Legal, Defence, and household brands, and has a notable track record of protecting people of interest during critical times.



ABOUT CYBIT:

Cybit is a trusted partner offering over three decades of technology expertise and specialisms in data analytics, AI, cybersecurity, modern workspace, hybrid cloud, and managed services. Cybit empowers private and public sector organisations to predict change, protect what matters, and perform with confidence.

At the heart of Cybit's approach is a belief that technology should do more than enable operations—it should unlock new opportunities, accelerate growth, and create a positive impact for people, communities, and the planet. By integrating intelligent, secure, and connected solutions, Cybit transforms complexity into clarity, helping clients stay ahead of threats, uncover actionable insights, and optimise performance at every level.

Cybit's collaborative ethos is reflected in its strong partnerships with leading technology vendors and its commitment to continuous improvement. Every solution is tailored to the

client's unique goals, delivered with integrity, and measured by real-world outcomes. Whether enabling smarter decision-making through data and AI, building resilient digital environments, or supporting sustainable business transformation, Cybit is dedicated to shaping a future where technology is a force for good. For more information about Cybit, please visit:

www.cybit.com

OUR VALUED PARTNERS



proofpoint.

Qlik

SOPHOS



CYBIT

Equinox House
Silver Fox Way,
Cobalt Business Park,
Newcastle Upon Tyne,
NE27 0QJ

03308 284838
hello@cybit.com

