CloudClevr

Can you prove your cyber security?

Cyber security isn't a destination.
It's a continual process of replacing assumptions with evidence.

Authors: Rob Smith and Simon du Plessis

cloudclevr.com

Contents

Chapter One

The confidence gap

Cyber security has become one of the fastest-growing areas of technology investment. Gartner forecasts worldwide end-user spending on information security to exceed $212 billion in 2025, an increase of more than 15% on the previous year. Few areas of enterprise technology have experienced the same level of sustained investment, reflecting a broader shift in which cyber security has moved from being a specialist IT concern to a strategic business priority.

That investment has undoubtedly strengthened organisational resilience. However, it has not eliminated one of the most fundamental challenges facing today's IT leaders. Security incidents continue to affect organisations of every size, despite record levels of spending.

The question is no longer whether organisations recognise the importance of cyber security, they clearly do. The more difficult question is whether they can demonstrate that their investment is delivering the level of protection they believe it is.

Identity management has become more sophisticated. Endpoint protection has evolved. Cloud security, security awareness training and continuous monitoring have become part of everyday operations rather than specialist projects. For many IT teams, cyber security is no longer a separate discipline; it is woven into almost every technology decision they make.

Against that backdrop, it would be reasonable to assume that organisations now have a much clearer understanding of their security posture than they did a decade ago.

In many respects, they do.

They know what technologies they have purchased. They know which controls have been deployed. They can often point to policies, dashboards and compliance reports that demonstrate considerable progress. Security has become more visible, more measurable and, in many organisations, more frequently discussed at board level than ever before.

Yet there is another reality that receives far less attention.

When organisations experience a significant security incident, the post-incident review rarely concludes that they cared too little about cyber security. More often, it uncovers a series of assumptions that had never been challenged. A backup had not been tested recently. A former employee still retained access to a business application. A monitoring alert had gone unnoticed. An AI tool had been adopted informally without anyone fully understanding how company information was being used.

None of these situations necessarily reflect poor practice or a lack of investment. They are often the natural consequence of managing increasingly complex environments where technology evolves faster than governance, and where operational priorities leave little time to validate every assumption.

This distinction between believing that controls exist and knowing that they are operating as intended is what we describe as the **confidence gap**.

The confidence gap is not a measure of technical capability. It is the difference between confidence and evidence.

For business leaders, this gap matters because it affects operational continuity, customer trust, regulatory confidence and the ability to make informed investment decisions.

An organisation may be highly confident that its backups would support recovery from a ransomware attack. Until those backups have been tested, however, that confidence remains an assumption.

An organisation may be confident that only authorised users have access to sensitive information. Until those permissions have been reviewed and validated, that confidence is based largely on trust.

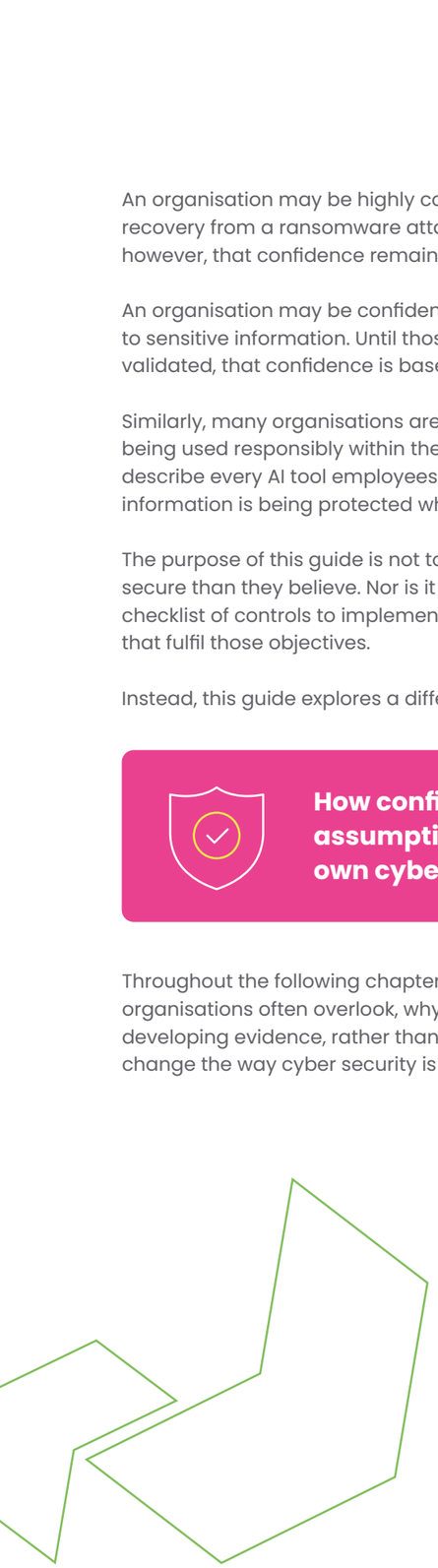
Similarly, many organisations are confident that artificial intelligence is being used responsibly within the business. Yet few could confidently describe every AI tool employees are using today or explain how sensitive information is being protected when those tools are used.

The purpose of this guide is not to suggest that organisations are less secure than they believe. Nor is it intended to provide another technical checklist of controls to implement. There are already countless publications that fulfil those objectives.

Instead, this guide explores a different question.

How confident should you be in the assumptions you make about your own cyber security?

Throughout the following chapters, we will look at the questions that organisations often overlook, why those questions matter, and how developing evidence, rather than simply confidence, can fundamentally change the way cyber security is understood across the business.



Chapter Two

The myth of visibility

There is an assumption that accompanies almost every investment in cyber security. It is rarely discussed because, on the surface, it appears entirely reasonable.

If an organisation has invested in modern security tools, surely it has a clear picture of what is happening across its environment?

After all, IT teams have access to more information than ever before. Dashboards present live security alerts, cloud platforms generate continuous telemetry, identity systems record every authentication attempt, endpoint protection tools monitor devices in real time and security operations centres can aggregate millions of events every day.

Visibility, it would seem, has never been better.

Yet having access to more information is not the same as having greater understanding.

The volume of information available has increased at a faster rate than the time available to interpret it. Every new platform introduces another dashboard, another set of alerts and another source of operational data. Rather than simplifying security, technology has often fragmented it across multiple tools, teams and suppliers.

This creates an interesting paradox.

Businesses have never before collected more security data, yet they have never been less certain that they are seeing the whole picture.

The issue is not that important information is unavailable. More often, it is hidden in plain sight.

An unused administrative account remains active because nobody has reviewed access permissions for several months. A business-critical application sits outside central monitoring because responsibility transferred between teams. Employees begin using a new AI tool because it helps them work more efficiently, yet no formal discussion ever takes place about how business information is being processed or stored.

Each of these situations appears relatively minor when viewed in isolation.

Together, they create blind spots and alter the organisation's risk profile.

Blind spots are not created because organisations ignore security. They develop because modern technology environments change continuously. New applications are introduced, suppliers change, mergers take place, projects finish, teams evolve, and employees discover new ways of working. Every change is entirely logical in isolation. Over time, however, those changes accumulate until the organisation's understanding of its own environment begins to diverge from reality.

This is one of the reasons why cyber security has become increasingly difficult to measure through technology alone.

The question is no longer,
"Do we have the right tools?"

It is, *"Do we understand what those tools are telling us, and just as importantly, what they may not be telling us?"*

Perhaps the greatest misconception in cyber security is that visibility is something an organisation either has or does not have.

In reality, visibility exists on a spectrum.

There are areas where organisations have excellent oversight. There are others where confidence is built largely on assumption. The challenge is identifying the difference before someone else does.

Artificial intelligence provides a timely example.

Across industries, businesses have invested heavily in securing corporate systems, yet relatively few can confidently explain which AI tools employees are using today. Fewer still could explain what information is being entered into those tools, whether appropriate safeguards exist, or how quickly new AI applications are appearing across the business.

The issue is not a lack of security products. It is a lack of visibility into changing behaviours.

The same principle applies across identity, data protection, supplier access and business applications. Technology continues to evolve, often far more quickly than governance processes. As a result, organisations can find themselves protecting yesterday's environment while today's environment quietly takes on a different shape.

Improving visibility therefore requires more than additional monitoring. It requires curiosity.

It requires organisations to continue asking questions, even in areas where confidence is already high. It requires IT teams to challenge assumptions, validate controls and periodically step back from the dashboards to ask a deceptively simple question.

"What might we not be seeing?"

That question is often where meaningful improvements begin.

Not because it immediately reveals hidden risks, but because it changes the mindset from monitoring technology to understanding the environment as a whole.

Ultimately, visibility is not measured by the number of dashboards an organisation owns. It is measured by how confidently it can explain what is happening across its technology estate, why it is happening, and whether that understanding is supported by evidence rather than assumption.

Chapter Three

Complexity is the new attack surface

Cyber security has traditionally been viewed as a technical discipline. Protecting the organisation meant deploying the right technologies, configuring them correctly and maintaining them effectively. The assumption was straightforward: stronger security controls would lead to stronger security outcomes.

For many years, that assumption was largely correct.

Today's challenge is different.

An average small to mid-sized organisation now juggles multiple security tools from different vendors to maintain their security posture. Rather than simplifying cyber security, this growing ecosystem can make it harder to maintain visibility, integrate controls and respond consistently across the environment. Organisations with fragmented security stacks were found to take an average of 72 days longer to detect threats and 84 days longer to contain them than those with more integrated environments.

Business applications are no longer confined to a single data centre or office network. Employees work from multiple locations, often using a combination of corporate and personal devices. Critical systems are spread across cloud providers, software-as-a-service platforms and third-party suppliers. Artificial intelligence is becoming embedded into everyday workflows, while collaboration tools allow information to move across organisational boundaries almost instantly.

Each of these developments has delivered enormous benefits. Organisations are more agile, employees are more productive, and technology has become far more accessible than ever before.

However, every improvement has also introduced another layer of complexity.

Even relatively small organisations are managing an environment that may include:

- Multiple cloud platforms and software-as-a-service applications.
- Employees working across corporate and personal devices.
- Third-party suppliers with varying levels of access.
- Collaboration platforms that allow information to move instantly between people and organisations.
- Artificial intelligence tools that are being adopted faster than formal governance can keep pace.

None of these developments are inherently problematic. In fact, most represent genuine progress. The challenge is that every new technology, application or integration changes the organisation's operating environment, often in ways that are not immediately visible.

Complexity, in itself, is not a weakness. It is simply a characteristic of modern technology. The challenge is that complexity creates opportunities for assumptions to develop unnoticed.

An identity platform may be working exactly as intended, yet an account created for a temporary project remains active long after the project has finished. A collaboration platform may be configured securely, while sensitive information is simultaneously being shared through an AI tool that sits entirely outside formal governance. A backup strategy may successfully protect critical infrastructure, while overlooking newer cloud services that have gradually become essential to the business.

None of these situations are typically the result of negligence.

More often, they are the consequence of change.

Technology evolves continuously, but governance tends to evolve periodically. Organisations implement new applications, integrate acquisitions, respond to customer demands and adopt new ways of working every day. Policies, reviews and audits happen much less frequently. Over time, a small but important gap begins to emerge between the environment organisations believe they are managing and the environment that actually exists.

This is one of the reasons why cyber security conversations increasingly focus on resilience rather than prevention.

The question is no longer whether organisations can prevent every attack. Few would claim that is realistic. Instead, resilience asks a more practical question:

How quickly can an organisation identify change, understand its impact and respond before it becomes a significant problem?

That shift in thinking changes the role of security. It is no longer a gatekeeper positioned at the edge of the network. It has become an ongoing process of understanding how people, technology and information interact within a constantly changing environment.

Every technology project, regardless of its objective, changes an organisation's risk profile in some way.

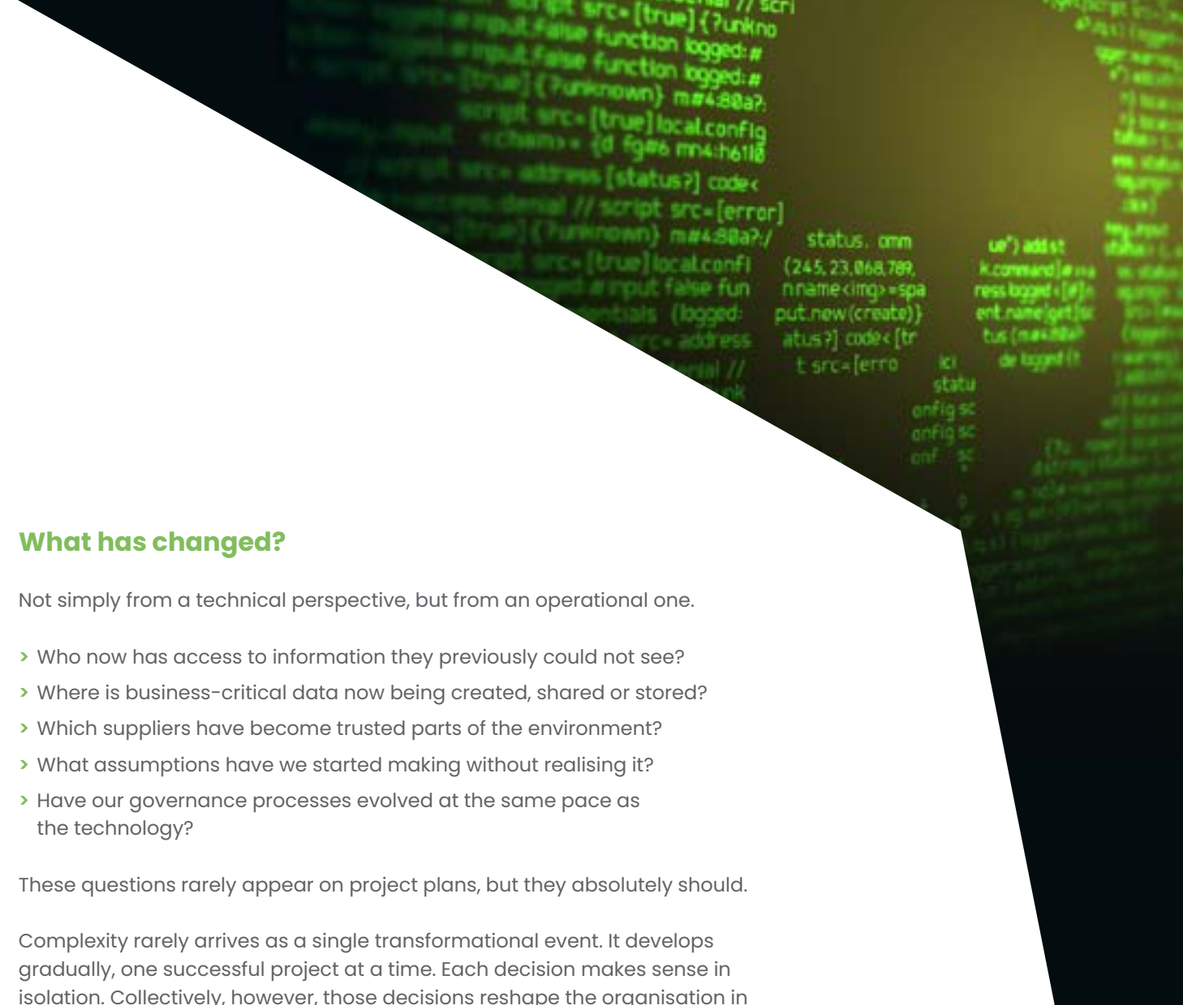
For example:

- A new collaboration platform changes how information is shared.
- A new supplier introduces additional trust relationships.
- A business acquisition creates new identities, devices and applications.
- A new AI tool changes where information is processed and how quickly it can be distributed.
- A new automation platform changes who, or what, can acces business data.

None of these changes are negative. But each one introduces new questions that organisations need to answer if they are to maintain confidence in their security posture.

This is not an argument against innovation. Quite the opposite. Innovation is essential. The challenge is recognising that every new capability should be accompanied by an equally deliberate conversation about visibility, ownership and accountability.

One of the most valuable questions an organisation can ask during any technology project is remarkably simple.



What has changed?

Not simply from a technical perspective, but from an operational one.

- Who now has access to information they previously could not see?
- Where is business-critical data now being created, shared or stored?
- Which suppliers have become trusted parts of the environment?
- What assumptions have we started making without realising it?
- Have our governance processes evolved at the same pace as the technology?

These questions rarely appear on project plans, but they absolutely should.

Complexity rarely arrives as a single transformational event. It develops gradually, one successful project at a time. Each decision makes sense in isolation. Collectively, however, those decisions reshape the organisation in ways that are often difficult to recognise until someone deliberately steps back to look at the whole picture.

The organisations that manage complexity most effectively are not necessarily those with the largest security teams or the biggest technology budgets. They are the organisations that regularly create time to reconnect strategy with reality. They recognise that technology will continue to evolve, and that their understanding of the environment must evolve alongside it.

Once complexity is understood, it becomes manageable. When it is ignored, it quietly becomes another attack surface.

Chapter Four

When good intentions create invisible risk

Every significant shift in workplace technology follows a familiar pattern.

A new tool emerges that promises to make work easier, faster or more productive. Early adopters begin experimenting with it, often outside formal processes. Teams discover new ways of solving everyday problems. Before long, what began as individual experimentation becomes part of normal working practice.

History suggests this is neither unusual nor unexpected. Email, cloud storage and collaboration platforms all became part of everyday working practices long before organisations fully understood how they should be governed, and artificial intelligence is following much the same path. The speed, however, is unlike anything organisations have experienced before.

Unlike previous technology shifts, employees do not need a project, a procurement process or formal approval to begin using AI. Many tools are available within seconds, often at little or no cost, and can immediately help with writing, analysing information, summarising meetings, creating presentations or solving technical problems.

That accessibility is one of AI's greatest strengths. It is also one of its greatest governance challenges.

This is not because employees are deliberately bypassing security controls. In most cases, they are trying to become more productive. They are looking for faster ways to complete repetitive tasks, communicate more effectively or make better use of their time.

The intention is positive. The visibility is not always there.

Research from Microsoft found that 71% of UK employees have used consumer AI tools at work, with more than half doing so every week. One of the most common reasons was simply that no approved alternative had been provided.

That finding is significant because it changes the nature of the conversation.

Shadow AI is often described as a security problem. In reality, it is just as much a business problem.

It raises questions that extend far beyond technology.

- Where is business information now being processed?
- Which AI tools have become part of everyday workflows?
- How are employees deciding what information is appropriate to share?
- Who owns responsibility for governing AI across the organisation?
- How quickly can new tools appear before anyone in IT becomes aware of them?

These are not hypothetical questions.

They are operational questions that many organisations are already trying to answer.

The challenge is that AI changes the relationship between people and information.

Historically, information moved between systems that the organisation largely understood and managed. Today, information can move into publicly available AI services, browser extensions, meeting assistants and specialist applications that may never have been reviewed by security or compliance teams.

That does not automatically mean information is being mishandled.

It does mean organisations have less certainty than they may realise about where sensitive information is travelling and how it is being used.

This is where the confidence gap begins to widen once again.

Many organisations are confident that employees understand their responsibilities around information security. Yet relatively few could confidently describe every AI-enabled service currently being used across the business, how frequently those services are being accessed or what safeguards exist around the information being shared.

The pace of adoption is simply moving faster than traditional governance.

Recent research highlights how quickly this gap can become a business issue.

IBM found that organisations experiencing security incidents involving Shadow AI incurred, on average, an additional $670,000 in breach-related costs, while 97% of organisations reporting AI-related breaches lacked appropriate AI access controls.

These findings should not discourage organisations from embracing AI.

AI has become an essential business capability. The question isn't whether organisations should adopt it, but how they can do so in a way that balances innovation with visibility and governance.

The organisations making the greatest progress are rarely those attempting to prohibit AI.

Instead, they are creating environments where employees have access to trusted, supported tools and clear guidance on how they should be used.

That typically includes:

- Providing approved AI platforms that meet security and compliance requirements.
- Helping employees understand what information should never be shared with public AI services.
- Ensuring appropriate roles and permissions are implemented across AI infrastructure to control what corporate data users have access to
- Monitoring AI adoption trends so governance evolves alongside usage.
- Treating AI as part of everyday cyber security discussions rather than a separate technology initiative.

Perhaps most importantly, they recognise that Shadow AI is not fundamentally about artificial intelligence.

It is about people.

When employees believe a new tool helps them work more effectively, they will naturally adopt it. If approved alternatives are unavailable or difficult to access, they will often find their own solution.

The responsibility, therefore, is not simply to govern AI. It is to create an environment where secure ways of working are also the easiest ways of working.

Ultimately, Shadow AI is not a story about technology moving too quickly. It is a story about organisations adapting to one of the fastest shifts in workplace behaviour they have ever experienced. Those that succeed will not necessarily be those with the most restrictive policies. They will be those that develop the visibility, governance and trust needed to embrace AI confidently, rather than simply reacting to it once it has already become embedded in the organisation.

Chapter Five

Cyber security is no longer an IT problem

There was a time when understanding an organisation's technology estate was a relatively achievable task. Most systems were purchased through IT, deployed by IT and supported by IT. If you wanted to know what technology existed within the organisation, there was usually one place to look and one team responsible for managing it.

But now, maintaining IT visibility is more challenging than ever. Today, technology is continuously adopted. New applications appear to solve business problems, improve productivity and respond to changing customer expectations. Increasingly, those decisions are made by the people closest to the challenge rather than the technology team responsible for governing it.

This is not a failure of governance. It is evidence of how deeply technology has become embedded in every part of modern business.

Technology is no longer something that sits alongside the organisation. It has become part of almost every process, every customer interaction and every employee's working day. As organisations become more digital, technology decisions naturally become more distributed.

That shift has created enormous opportunities for innovation, collaboration and productivity. It has also fundamentally changed the nature of cyber security.

Research from Gartner suggests that by 2027,

75% of employees will acquire, modify or create technology outside traditional IT visibility, reflecting the continued growth of business-led technology and citizen development.

Rather than seeing technology as something provided exclusively by IT, organisations are increasingly enabling departments and individuals to solve problems for themselves.

This trend should not be viewed negatively.

Quite the opposite.

The most successful transformation initiatives begin because people closest to the business identify better ways of working. Marketing teams adopt platforms to improve customer engagement. Finance teams introduce new planning and reporting tools. HR teams invest in employee experience platforms. Operations automate repetitive tasks. Employees experiment with AI to improve productivity or reduce administrative effort.

These decisions are usually made with positive intent. They are designed to improve outcomes rather than introduce risk.

The challenge is that every technology decision also becomes a security decision, whether it is recognised as such or not.

A new application may process customer information differently. An AI assistant may analyse commercially sensitive documents. A third-party supplier may require access to internal systems. A workflow automation may connect multiple business platforms that were never previously linked together.

Individually, each decision appears relatively small. Collectively, they reshape the organisation's technology landscape.

This is why cyber security can no longer be viewed solely through the lens of infrastructure, devices and applications. It is influenced by business decisions, procurement decisions, operational decisions and everyday employee behaviour.

That represents an important shift in responsibility.

It does not mean everyone becomes responsible for cyber security in the technical sense. Few organisations would expect every employee to understand identity architecture or security operations.

It does mean that everyone has a role in protecting information and reducing unnecessary risk.

- Leadership teams define the organisation's appetite for risk and ensure cyber security remains part of wider business strategy.
- IT and security teams create secure foundations, provide governance and enable the safe adoption of new technologies.
- Business leaders ensure new ways of working are introduced responsibly within their own teams.
- Employees make informed decisions about the information they handle, the technologies they use and the way they adopt emerging tools such as artificial intelligence.
- Suppliers become trusted extensions of the organisation and increasingly form part of its overall security posture.

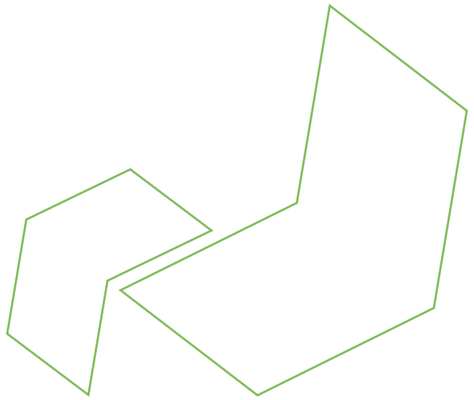
These responsibilities are different. They are also interdependent.

This is one of the reasons the language around cyber security is beginning to change.

For years, conversations focused primarily on technology.

- Endpoint Detection and Response
- Zero Trust
- Identity Management
- Security Operations
- Threat Intelligence

These technologies remain essential.



However, they are not the questions most leadership teams ask.

Business leaders are more likely to ask:

- How resilient are we if something goes wrong?
- Are we protecting our customers' information appropriately?
- Could this disrupt our operations?
- Are we meeting our regulatory obligations?
- Can we demonstrate that we are managing cyber risk responsibly?

These are business questions. Technology provides part of the answer, but not all of it.

This is where evidence becomes increasingly important.

It is relatively straightforward to explain which technologies have been deployed.

It is far more valuable to demonstrate that those technologies are operating effectively, adapting as the organisation changes and continuing to reduce risk over time.

One describes activity. The other demonstrates assurance.

As organisations continue to embrace cloud services, artificial intelligence and increasingly distributed ways of working, the relationship between technology and the business will become even more closely connected.

The organisations that thrive will not necessarily be those with the largest security budgets or the most sophisticated technology stacks.

They will be the organisations that recognise cyber security as a shared organisational capability rather than a specialist technical function.

Ultimately, cyber security is no longer about protecting technology.

It is about enabling people to adopt technology confidently, responsibly and securely as the organisation continues to evolve.

Chapter Six

From confidence to evidence

Throughout this guide, we have explored how cyber security has changed over the last decade. We have looked at the growing complexity of modern technology environments, the challenge of maintaining visibility across increasingly distributed organisations, the rapid adoption of artificial intelligence and the way responsibility for technology has expanded far beyond the IT department.

There is a common thread running through each of these changes.

Organisations have never had access to more sophisticated technology, more security tooling or more information about their environments than they do today. At the same time, however, they have never had to manage such a rapidly changing technology landscape. The result is that confidence can sometimes outpace certainty. Organisations often believe they understand their security posture, yet struggle to demonstrate that confidence with evidence when they are asked to do so.

This distinction matters because expectations have changed.

Customers increasingly expect reassurance that their information is being protected appropriately. Regulators want organisations to demonstrate accountability. Cyber insurers want evidence that appropriate controls are in place, while leadership teams need confidence that cyber security is supporting operational resilience rather than introducing unnecessary business risk.

None of these stakeholders are asking organisations to eliminate every possible risk. They understand that technology, like every aspect of modern business, involves uncertainty. What they increasingly expect is that organisations understand their own environment, recognise where their greatest risks exist and can demonstrate that appropriate controls are operating effectively.

That represents a subtle but important shift in how cyber security is measured.

Success has traditionally been defined by implementation. Organisations invested in new technologies, introduced new policies and completed projects designed to strengthen their security posture. Those activities remain important, but they are no longer sufficient on their own. Increasingly, organisations are judged not simply on what they have implemented, but on whether they can demonstrate that those controls continue to operate effectively as the organisation evolves.

One of the simplest ways to understand this change is to consider the questions organisations ask themselves.

Instead of assuming...	Consider asking...
We have backups, don't we?	When did we last test our ability to recover from them?
Everyone uses multi-factor authentication.	How do we know every privileged account is consistently protected?
We don't have a Shadow AI problem.	What evidence supports that conclusion?
We monitor our environment.	How quickly would we identify unusual behaviour if it occurred today?
Our suppliers are secure.	When did we last review the access they have to our systems and information?

The difference between these questions is subtle, but significant. The first seeks reassurance that something exists. The second seeks evidence that it is working as intended. That shift in thinking encourages organisations to move beyond assumptions and towards a culture of continuous validation.

Perhaps the most reassuring aspect of this approach is that it rarely depends on significant new investment. More often, it depends on developing better organisational habits.

The organisations that consistently improve their cyber resilience are not necessarily those purchasing the largest number of security products; they are the organisations that regularly challenge assumptions, review existing controls and remain curious about how their technology environment is changing.

In practice, that often means creating opportunities to pause and ask questions that day-to-day operational pressures rarely leave time for.

For example:

- Are our existing controls still appropriate for the way our organisation works today?
- Have new technologies, suppliers or AI tools changed our risk profile?
- Are we relying on assumptions that have never been validated?
- Could we demonstrate our current security posture if a customer, insurer or regulator asked us tomorrow?
- Have our governance processes evolved at the same pace as the technology they are intended to support?

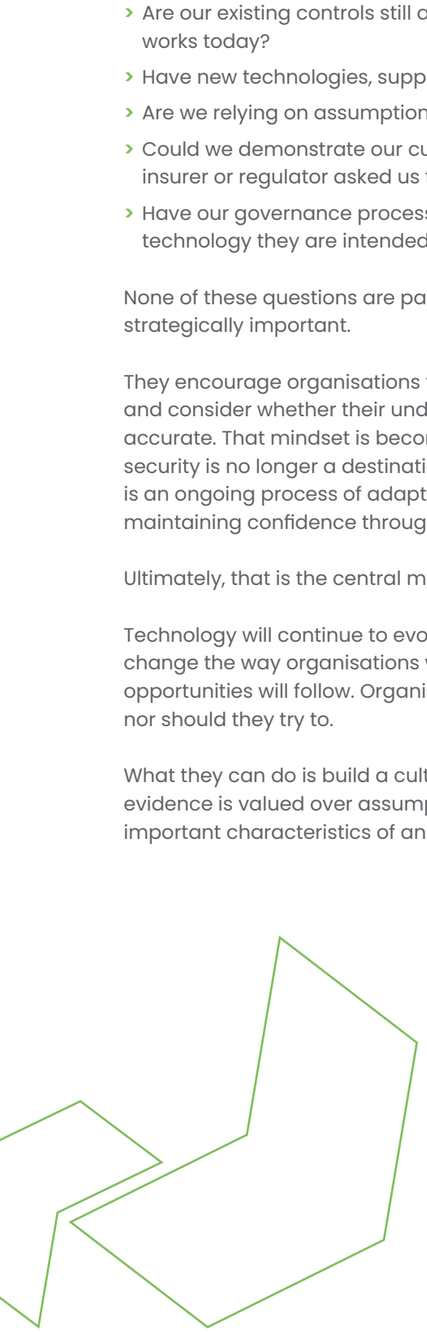
None of these questions are particularly technical. They are, however, strategically important.

They encourage organisations to step back from the operational detail and consider whether their understanding of the environment remains accurate. That mindset is becoming increasingly valuable because cyber security is no longer a destination that organisations eventually reach. It is an ongoing process of adapting to change, validating assumptions and maintaining confidence through evidence rather than familiarity.

Ultimately, that is the central message of this guide.

Technology will continue to evolve. Artificial intelligence will continue to change the way organisations work. New threats will emerge, and new opportunities will follow. Organisations cannot predict every change, nor should they try to.

What they can do is build a culture in which confidence is regularly tested, evidence is valued over assumption and curiosity becomes one of the most important characteristics of an effective cyber security strategy.



Where do you go from here?

If there is one message that runs consistently throughout this guide, it is that cyber security has become less about implementing individual technologies and more about understanding how those technologies, people and processes work together.

That is both the challenge and the opportunity facing organisations today.

Over the past decade, businesses have invested heavily in strengthening their cyber security. New tools have been deployed, governance has improved, and cyber risk has rightly become a regular topic of discussion at board level. These developments have made organisations significantly more resilient than they were even a few years ago.

At the same time, the environment those controls are designed to protect has continued to evolve.

Technology is changing more quickly than ever before. Artificial intelligence is reshaping the way people work. Employees expect greater flexibility. Business applications continue to multiply, and suppliers increasingly form part of the extended technology ecosystem.

The result is that cyber security has become a moving target. It is no longer enough to ask whether controls have been implemented. Organisations increasingly need to understand whether those controls continue to reflect the reality of how people work today.

How do we know?

- How do we know our visibility is complete?
- How do we know our governance has kept pace with technology?
- How do we know our assumptions remain valid?
- How do we know we could demonstrate our cyber security posture if we were asked to do so tomorrow?

These are not questions with permanent answers. They are questions that should be revisited regularly as organisations continue to evolve.

Perhaps that is one of the most important changes in modern cyber security.

The objective is no longer to reach a point where security is “finished”. Instead, the objective is to build the confidence that comes from continually validating, reviewing and improving the organisation’s understanding of its own environment.

So, how confident are you?

Throughout this guide we’ve explored some of the questions that organisations are increasingly asking themselves.

Now it is an opportunity to consider those questions in the context of your own organisation.

We’ve created a short **Cyber Confidence Quiz** to help you do exactly that.

It takes around five minutes to complete and has been designed to encourage reflection rather than test technical knowledge. Based on your responses, you’ll receive a personalised Cyber Confidence Report that highlights areas where confidence appears well founded, identifies topics that may be worth exploring further and provides practical recommendations to help strengthen your security posture.

The report is not intended to provide a definitive assessment of your organisation’s cyber security. Rather, it is designed to help answer a much simpler question.

How confident should you be in the assumptions you make today?

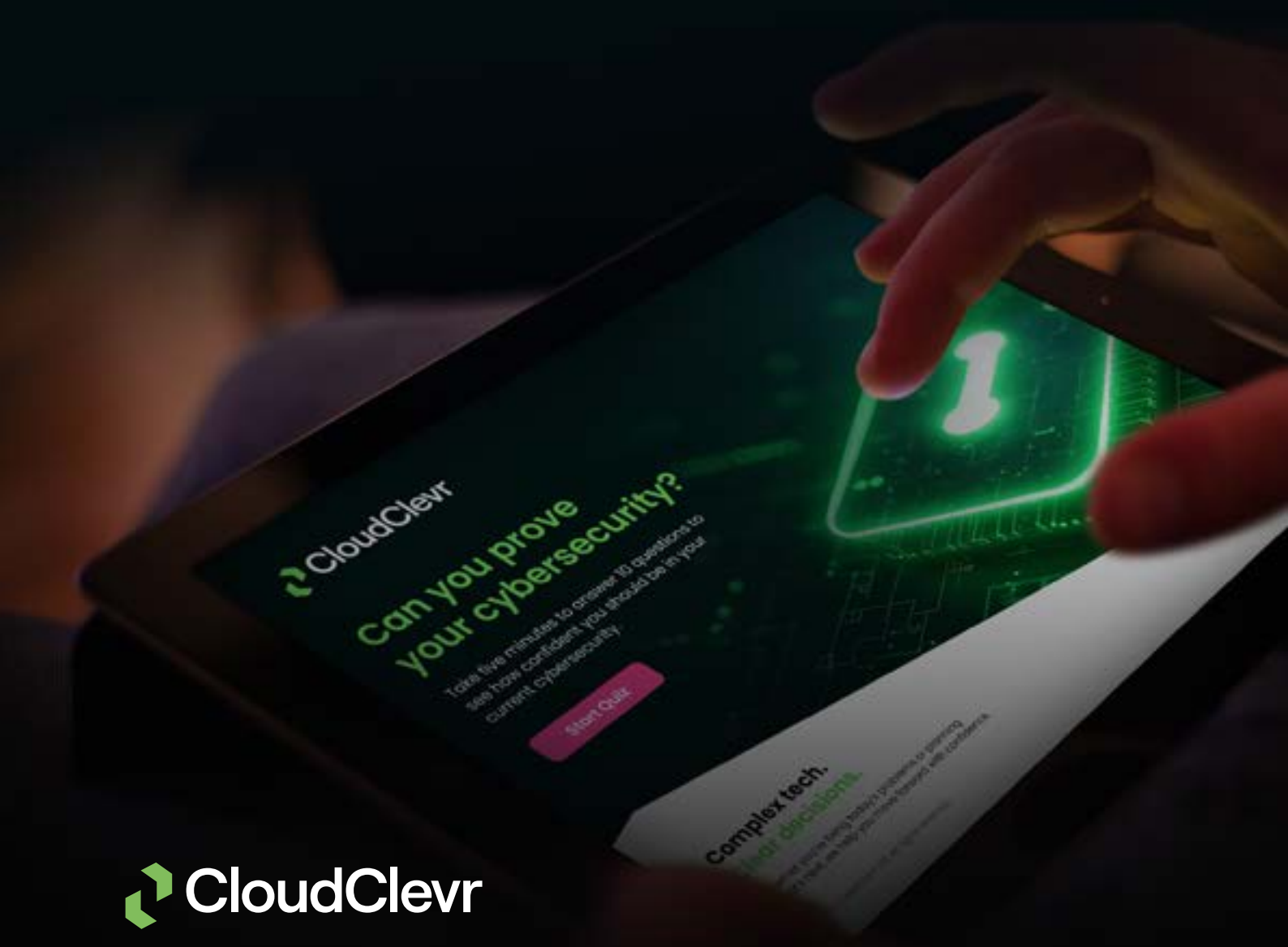
Whether your report confirms your confidence or highlights opportunities to strengthen it, we hope it provides a useful starting point for conversations within your own organisation.

Because the most valuable outcome of any cyber security programme is not simply deploying better technology.

It is developing a better understanding of the environment you are trying to protect.

Take the Cyber Confidence Quiz

- Answer ten questions.
- Receive your personalised Cyber Confidence Report.
- Discover where confidence is supported by evidence, and where there may be opportunities to strengthen it.



CloudClevr

cloudclevr.com