HIDDEN™ Framework Guide

A Complete Guide to Making your Cyber Risk Visible

Cyber security doesn’t fail overnight, gaps build over time

Cyber security doesn’t fail because businesses don’t care about it.
It breaks down because, over time, it becomes complex, reactive, and fragmented.

Most businesses feel they are reasonably well protected.

You may already have security tools in place. Someone is responsible. Controls exist across different parts of the organisation.

But when you step back, it can still be difficult to answer a simple question:

Are we actually secure, and can we prove it?

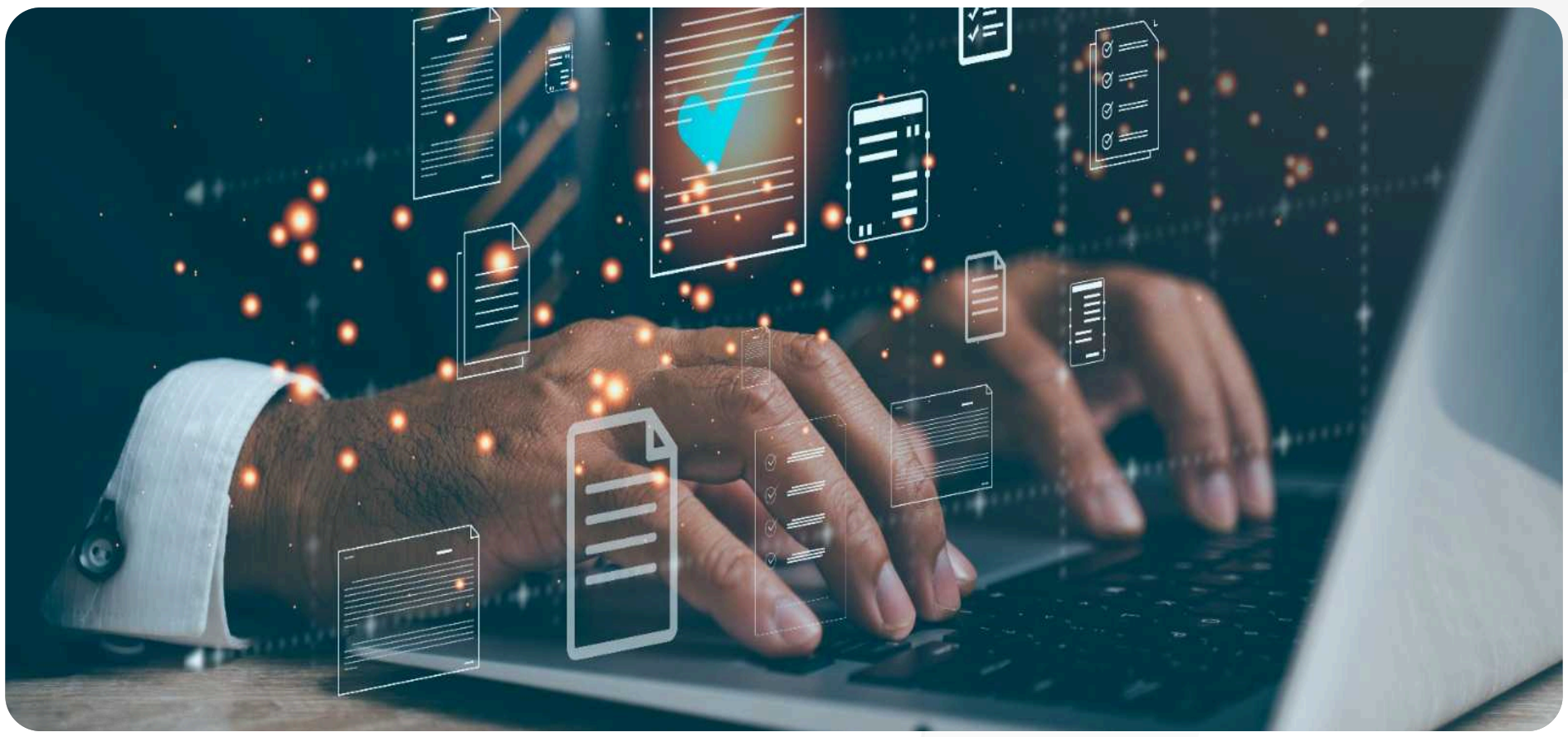
That uncertainty is where many SMBs find themselves.
Security is often managed in fragments: one tool at a time, one issue at a time, one decision at a time. There is no single, clear view. No shared language. And no easy way to understand where you are strong, where you are exposed, and what to prioritise next.

This doesn’t happen because of poor decisions.

It happens because of sensible decisions made reactively or in isolation — adding tools, solving problems, responding to risks. But over time, those choices create gaps that are difficult to see.

That’s the gap HIDDEN™ is designed to solve.

This guide explains how the HIDDEN framework helps you move from scattered tools and reactive fixes to a structured, measurable cyber security programme, so you can see clearly, act with confidence, and improve over time.



Reasons Current SMB Cyber Security Approaches Fail

Developing a robust cyber security strategy is easier said than done, as SMBs face a set of recurring challenges, many of which build gradually after a while.

Cyber risk increases faster than controls
The approach to attacks on businesses are constantly evolving, while security setups often stay the same. What worked 12–18 months ago may no longer be sufficient today.

Leaders struggle to see value from cyber spend
Even with investment in tools and services, it can still be difficult to answer a simple question:

“Are we actually protected?” Without a clear view, security can feel like a cost, rather than something that delivers measurable value.

Skills gaps
Many SMBs rely on one or two IT professionals responsible for everything. Security becomes just one of many competing priorities.

Compliance pressure
Cyber insurers, regulators, and enterprise customers increasingly expect evidence of security maturity, not assumptions.

Weak recovery readiness
Backups, access controls and device protections may all exist. But in real incidents, organisations often discover gaps (especially if those controls haven’t been tested under pressure).

Individually, these challenges are manageable. But together, they can create exposure across the organisation, often in ways that aren’t immediately visible.

HIDDEN exists to make those risks visible and manageable by providing:

- A clear framework
- A shared language between IT managers and leadership for discussing risk
- A roadmap for continuous improvement
- Measurable outcomes over time

Why HIDDEN™ Was Born

Short answer?
Because most businesses struggle to see or prove how secure they really are.

Because you can’t fix what you can’t see.

Before HIDDEN, every security engagement looked different. But we found ourselves solving the same problems over and over again with our customers.

Businesses often had:

- Firewalls but weak access controls
- Antivirus but no visibility into user behaviour
- Backups that had never been tested
- Endpoint alerts that no one had time to review
- An IT manager singlehandedly firefighting around the clock with no time to improve security

In other words, cyber security had gone rogue:

- Tools were purchased after incidents.
- Policies were written after audits.
- Decisions were made in isolation.

This meant environments were expensive, fragmented, difficult to justify to leadership, and worst of all, impossible to measure.

No matter the sector, size, or ‘tech stack’, the same six gaps kept showing up. Each and every single time.

The risk wasn’t just in the tools themselves: it was in the gaps between them.

That’s when it became clear:
Most SMBs don’t need more products (they’ve got enough as it is), They need a framework to follow.

Something simple, structured, and easy to understand. Something that turns cyber security into a programme, rather than a collection of disconnected solutions.

HIDDEN isn’t another product or tool; it’s a way to make sense of what you already have.

Customer Story

We worked with a 70-employee professional services firm. They believed they were secure because they had antivirus software, a firewall, and backups in place.

Then they were hit by ransomware.

Several issues emerged quickly:

- The malware bypassed antivirus detection
- The attack entered through a user account
- Backups had not been tested for nearly a year

When the company attempted recovery, the backups failed.

Despite having all those tools in place, they weren't recoverable.

It took nine days to get the business operational again.

When we assessed their environment against the HIDDEN framework, every layer of security had a gap, the kind that usually stays HIDDEN (pun intended) until it's too late.

The lesson was simple: **backups aren't protection if they don't recover**, and recovery must be tested, monitored, and governed.

What is the HIDDEN™ Framework?

What this Framework delivers:

HIDDEN is a simple framework that gives you a clear, shared view of your cyber security across six critical areas of your business, so IT teams and leadership can understand risk in the same way, and act on it with confidence.

It helps you see where you're exposed, know what to fix next, and track whether you're actually improving.

The framework answers six simple questions:

- Are your people strengthening your security, or putting it at risk?
- Do you have control over who can access what, and should they?
- Is your critical data protected, controlled, and used safely?
- If something went wrong, could you recover quickly and confidently?
- Are your devices secure, up to date, and under control?
- Is your network and cloud environment configured safely, or quietly exposed?

Rather than starting with technology, HIDDEN focuses on what actually matters: **the outcomes you need and the capabilities required to support them**. It centres on the core controls every organisation needs to operate securely.

For many organisations, the starting point is a **Cyber Security Snapshot**.

This is a simple, fast assessment that gives you an initial view of where you stand: highlighting obvious gaps, validating what's working, and pointing to where to focus first.

From there, the **HIDDEN Profile** brings everything together into a single, clear picture.

So you can instantly see:

- Where you're strong
- Where you're exposed
- Where your biggest risks sit
- And how balanced your overall security really is

Instead of relying on assumptions or scattered reports, you have one view that anyone in the business can understand.

Who we built this for:

Are you a business that is dealing with the following?

- Limited in-house security expertise
- A small IT team responsible for everything
- Technology decisions being made reactively
- Security investments that are difficult to justify
- Little visibility into where risk actually sits across the business

If so, the HIDDEN framework was built for you.

How we bring it to life:

So what does this actually look like in practice? Once you have a clear view of your security, the next step is turning that insight into meaningful progress. Most organisations move through a similar journey: from understanding where they stand, to improving, operating, and continuously evolving their security over time.

It typically looks like this:

1. Establish clarity
Start by understanding your current position. This means identifying where gaps exist, how your controls are performing, and where your biggest risks sit. Move from: “I don’t know where our gaps are.” To: “We understand our current security posture.”

2. Put the fundamentals in place
With that clarity, you can focus on strengthening the areas that matter most.
This is about addressing key risks, improving core controls, and making sure the basics are working as they should. Move from: “We know what’s wrong.” To: “We’re fixing the fundamentals.”

3. Make security part of how you operate
Once the foundations are in place, the focus shifts to consistency. Security becomes something that is monitored, maintained, and embedded into day-to-day operations , not something that’s revisited only after an issue arises. Move from: “Security is a project.” To: “Security is part of how we operate.”

4. Improve and adapt over time
As your business evolves, so do the risks you face. This stage is about continuously reassessing, improving, and demonstrating progress, so you’re not just maintaining security, but strengthening it over time. Move from: “We have security tools.” To: “We can demonstrate security maturity.”

How This Guide Will Help

This guide is designed to help business leaders and IT professionals:

Understand the six critical layers of cyber security

- **Identify common security gaps**
- **Ask the right diagnostic questions about risk**
- **Learn what “good” looks like for each layer**
- **Discover practical ways to improve over time**

By the end of this guide, you should have a clearer view of where your organisation stands today, and where to focus next.

Let’s dive in.

The Six HIDDEN™ Layers

H — Human Risk

HIDDEN™

In HIDDEN, this is where risk often starts: people.

Goal: Turn your employees from the organisation's largest security vulnerability into its strongest line of defence.

Most cyber incidents don't begin with a sophisticated technical exploit. They begin with a moment of trust: a convincing phishing email, a rushed click on a malicious link, or a file shared with the wrong recipient. In other words, **cyber security starts with people.**

But this isn't about pointing fingers. It's about understanding behaviour, and building habits that keep your people and your business safe.

Attackers increasingly rely on social engineering techniques designed to exploit human behaviour rather than technical vulnerabilities. Email impersonation, attempts to steal login details, and payment diversion scams are all examples of attacks that target people rather than systems.

At the same time, many organisations still treat security awareness as a compliance activity rather than an operational capability. A once-a-year training exercise that's completed and then forgotten about until it's time to do it again.

Employees may receive occasional training, but without ongoing visibility, it's difficult to understand how behaviour is changing across the organisation.

- Which teams are most vulnerable to phishing attacks?
- Which employees repeatedly click on malicious links?
- Which departments are more likely to expose sensitive information?

These questions are often difficult to answer with confidence. As a result, security teams are left reacting to incidents, instead of preventing them.

The Human Risk area of the HIDDEN framework focuses on turning security awareness into a continuous, measurable capability.

This includes building a culture where employees are equipped to recognise threats, report suspicious activity, and contribute actively to the organisation's security posture. By making behavioural risk visible and measurable, organisations can move from reactive awareness training to proactive risk reduction.

What Good Looks Like

In organisations with strong human risk management:

- Security awareness is part of everyday behaviour, not a one-off activity.
- Employees regularly participate in realistic phishing simulations.
- Behavioural risk is visible across teams and departments.
- Reporting suspicious activity is simple and encouraged.

Over time, employees develop the confidence to question unusual requests, verify unexpected communications, and raise concerns when something doesn't feel right. Instead of being the weakest link, your people become an active layer of defence.

Ask yourself:

- How many phishing simulations have you run in the last six months?
- Do you know which users or teams represent the highest behavioural risk?
- How do employees report suspicious activity today?

If these are difficult to answer, Human Risk may currently be a HIDDEN risk in your organisation.

Additional Resources

Articles:

Why Your Employees Are Your Biggest Security Risk
Traditional vs Human Risk Management: Which is Best for You?
How Do You Actually Measure Human Risk in Your Business?

While human behaviour is often the starting point for cyber incidents, attackers rarely stop there. Once credentials are compromised, they attempt to access systems using valid login credentials.

I — Identity Management

HIDDEN™

In HIDDEN, identity is where hidden access risk builds over time.

Goal: Ensure only the right people can access the right systems, in the right way, at the right time.

Today, attackers don't always break into systems. More often, they log in.
As organisations adopt cloud platforms, SaaS (software-as-a-service) applications, and hybrid working models, the way people access systems has fundamentally changed.

Employees now connect to the apps, data, and services they need to do their jobs from different devices, in different locations, and across different networks (often all within the same day).

In that environment, confirming that someone is who they say they are — securely and consistently, wherever they are — has never been more important.

This is why identity has effectively become the new 'security perimeter'. However, identity management often evolves organically over time. New accounts are created. Access permissions change. Privileges are granted temporarily, and not always removed.

Gradually, this creates an environment where access control becomes fragmented and difficult to manage.

Without structured identity governance, organisations often accumulate:

- Unused accounts belonging to former employees
- Excessive administrative privileges
- Inconsistent authentication policies across systems

These issues often remain unnoticed until something goes wrong. When login details are compromised (through phishing, password reuse, or other attacks), attackers can move through systems using valid credentials, often without triggering traditional security controls.

The Identity Management area of HIDDEN focuses on establishing structured, governed access control.

By strengthening authentication and controlling privileged access, you reduce the likelihood of unauthorised access, and limit its impact if it occurs.

What Good Looks Like

In organisations with mature identity governance:

- Multi-factor authentication (MFA) is enforced across users and administrators.
- Authentication is adaptive and risk-aware.
- Privileged access is tightly controlled and regularly reviewed.
- Joiner–mover–leaver processes are defined and consistently applied.
- Access rights are kept up to date and removed when no longer needed.

Identity becomes a visible, governed part of daily operations, not something that changes over time.

Ask yourself:

- Do all users and administrators have MFA enforced?
- How often are privileged accounts reviewed?
- What is your process for joiners, movers, and leavers?

If these are difficult to answer, Identity Management may be a HIDDEN risk in your organisation.

Additional Resources

Articles:

The 5 Essential Security Tools Your SMB Needs to Have

Strong identity governance helps control who can access systems. However, once access is granted, organisations must also ensure that the information within those systems is properly protected and maintained.

D — Data Controls

HIDDEN™

In HIDDEN, data risk is often about visibility: knowing what exists and who can access it.

Goal: Ensure sensitive information is visible, governed, and protected without slowing down productivity.

Data is one of your most valuable assets.

From financial records and customer information to intellectual property and operational data, your business relies on information to function and remain competitive. But the way data is created, shared, and used has changed significantly.

It now moves rapidly across email, collaboration platforms, cloud environments, and increasingly through AI-driven tools.

As data flows between people, devices, networks, and AI systems, maintaining visibility and control is essential. Otherwise, AI tools can surface inaccurate information or expose sensitive data in ways that were never intended.

So, while these technologies have streamlined productivity, they also create new security challenges.

Many organisations struggle to answer fundamental questions about their data:

- Where does sensitive information reside?
- Who has access to it?
- How is it being used or shared?

Without that visibility, data can be exposed through:

- Accidental sharing
- Misconfigured permissions
- Compromised accounts

The Data Controls area focuses on creating structured visibility and governance around your information.

By identifying sensitive data and applying appropriate controls, you can protect it without disrupting how your business operates.

What Good Looks Like

In organisations with strong data governance:

- Sensitive information is identified and classified.
- Data discovery tools provide visibility across the environment.
- Clear policies guide how information is shared.
- Data loss prevention (DLP) controls reduce the risk of exposure.
- Collaboration remains productive, but governed.

Instead of restricting productivity, data governance enables confident collaboration.

Ask yourself:

- Do you know where your sensitive data lives today?
- Who has access to it?
- Do you have controls preventing accidental data leakage?

If these are difficult to answer, Data Controls may be a HIDDEN risk in your organisation.

Additional Resources

Articles:

Is Your Data Helping or Hurting You? Here's How to Find Out

What You Need to Know About Data Loss Prevention (DLP)

Protecting sensitive information is critical, but your organisation must also be prepared for the possibility that systems may fail or be compromised. Even with strong security controls, incidents can still happen.

D — Disaster Recovery

HIDDEN™

In HIDDEN, recovery risk is often hidden in assumptions.

Goal: Ensure your organisation can recover quickly and confidently from incidents or failures.

Many organisations believe they are protected because they have backups in place.
But backups alone don’t guarantee recovery.

During incidents such as ransomware attacks, backup systems may be targeted, corrupted, or found to be incomplete.

In other cases, backups exist, but haven’t been tested.

These situations often reveal a key assumption: that recovery capability exists simply because backups are present.

In reality, recovery depends on:

- How quickly systems can be restored.
- Whether backups are usable.
- Whether processes are defined and tested.

Without this, downtime can be longer and more disruptive than expected.

The Disaster Recovery area focuses on ensuring recovery capabilities are reliable, tested, and aligned with your business needs.

What Good Looks Like

In organisations with mature disaster recovery:

- Backups are monitored and protected.
- Recovery processes are documented and tested.
- Critical systems are prioritised.
- Incident response plans are clearly defined.
- Leadership understands recovery expectations.

Confidence comes from testing, not assumption.

Ask yourself:

- When was your last successful restore test?
- If ransomware struck today, what would your recovery process be?
- What downtime could the business realistically tolerate?

If these are difficult to answer, Disaster Recovery may be a HIDDEN risk.

Additional Resources

Articles:

Why Do I Need Cyber Security Backup if I Have Microsoft 365?

How Acronis Fills in the Backup Gaps

Even with strong recovery capabilities, preventing incidents in the first place remains a priority. Many cyber attacks begin by exploiting vulnerabilities on user devices.

E — Endpoint Protection

HIDDEN™

In HIDDEN, risk appears when devices are managed differently across the business.

Goal: Create a consistent and secure baseline across all devices.

Every device connected to your systems and data represents a potential entry point for cyber criminals.

Laptops, mobile devices (both company-owned and personal), servers, and workstations are all doorways into the business.

In many SMB environments, endpoint security is handled in different ways across the organisation:

- Devices may run different operating systems.
- Security configurations can vary between teams.
- Laptops are often managed very differently from mobile devices.

As employees work across multiple devices, locations, and networks, this lack of consistency creates gaps that are difficult to see (but easy to exploit). For example, patching may depend on manual processes that take time, and security tools may generate alerts that are never fully investigated.

This is what attackers take advantage of: once they gain access to an endpoint, they can move laterally, escalate privileges, and access sensitive systems.

The Endpoint Protection area focuses on creating consistency, visibility, and control across all devices.

What Good Looks Like

- All devices follow a consistent security configuration baseline.
- Systems are regularly patched.
- Endpoint activity is monitored.
- Alerts are reviewed and acted on.

Over time, organisations can detect and respond to threats earlier, before they escalate.

Ask yourself:

- Who is actively monitoring your endpoints today?
- How quickly would you detect a threat?
- When were endpoint alerts last reviewed?

If these are difficult to answer, Endpoint Protection may be a HIDDEN risk.

Additional Resources

Articles:

EDR vs MDR vs XDR: A Comprehensive Comparison

MDR Not Meeting Expectations? Here's What's Really Going Wrong

SOC-as-a-Service: Busting the 'Too Small to Target' Myth

How MDM Can Bridge the Gap Between Zero Trust and BYOD

While endpoint security protects individual devices, attackers often attempt to move across the infrastructure once they gain access.

N — Network & Cloud Security

HIDDEN™

In HIDDEN, risks grow when systems change, rules build up, and visibility is lost over time.
Goal: Ensure your infrastructure remains secure, monitored, and well-governed over time.

Modern environments are increasingly complex.
Applications run in the cloud. Employees work from multiple locations.
As they work on the go, devices connect across office networks, home WiFi, mobile connections, and public networks.

While this enables flexibility, it also expands your attack surface.

Infrastructure often evolves organically:

- Firewall rules accumulate.
- Cloud configurations change.
- Networks expand as new systems are introduced.

Without structured governance, this can lead to unseen weaknesses:

- Networks may lack segmentation.
- Configurations may become more complex.
- Access paths may remain open longer than intended.

Again, these issues often remain unnoticed until an incident occurs.

The Network & Cloud area focuses on visibility, monitoring, and governance across your infrastructure.

What Good Looks Like

- Networks are segmented appropriately.
- Firewall rules are reviewed regularly.
- Cloud configurations are monitored.
- Suspicious activity is visible.

Security becomes a continuous process, not a one-time setup.

Ask yourself:

- How confident are you in your firewall and cloud configurations?
- Is your network segmented, or is it flat?
- Who monitors your cloud environment?

If these are difficult to answer, Network & Cloud Security may be a HIDDEN risk.

The Full Picture: Completing the HIDDEN™ Framework

Each area of the **HIDDEN** framework addresses a critical part of your organisation's cyber resilience:

- **Human Risk** strengthens behaviour and awareness
- **Identity Management** controls access to systems
- **Data Controls** protect your information
- **Disaster Recovery** ensures you can recover
- **Endpoint Protection** secures your devices
- **Network & Cloud Security** protects your infrastructure

Individually, each layer matters.

Together, they give you something far more valuable: a **complete, structured view of your cyber security**. Instead of looking at isolated tools or individual controls, you can see how everything connects, and where the gaps may exist. But understanding your security is only the first step. Cyber security isn't something you complete once and move on from.
It's something that either improves over time, or quietly slips out of sync.

Measuring Your Strength and Building a Cyber Roadmap

Many organisations invest in cyber security but still find it difficult to demonstrate progress. You may have tools in place.

You may have processes defined. But without a clear way to measure improvement, it's hard to know whether things are actually getting better.

This is where HIDDEN adds a different layer of value.

By assessing your organisation across all six layers, HIDDEN gives you a structured way to:

- Benchmark your current position
- Identify where your biggest risks sit
- Prioritise what matters most
- Track how your security improves over time

This is reflected through your **HIDDEN Profile**: a clear, visual representation of your security across all areas.

Instead of relying on assumptions or scattered reports, you have:

- One view of your overall security
- A shared understanding across IT and leadership
- A way to demonstrate progress over time

Metrics often include:

- Phishing susceptibility trends
- Identity protection coverage
- Endpoint compliance
- Backup restore success
- Incident response time

This shifts cyber security from something that feels theoretical — to something you can clearly measure, track, and communicate.

See where you could be exposed

Start your **Cyber Security Snapshot** to get a clear view of where you are strong vs where you are exposed across those six critical areas.

Are your people a weak point?	84%	Low Risk
Do you have controls aroun…	72%	Medium…
How is your data governed?	38%	High Risk
Can your business recover i…	64%	Medium…
Are your devices a risk to yo…	50%	Medium…
Is your internet access prot…	68%	Medium…

Next Steps

If parts of this guide feel familiar, you're not alone.

Most organisations don't lack tools or intent. They lack a clear way to see how everything fits together, and whether it's working as expected.

That's the starting point. Before making changes, adding tools, or investing further, the most valuable thing you can do is understand where you stand today.

A **Cyber Security Snapshot** gives you that clarity. It helps you understand:

- Where your current security position sits
- Which areas may represent the highest risk
- What your next steps should be

So instead of guessing or reacting you can move forward with confidence

See where you could be exposed

Start your Snapshot >