Cyber Maturity:

Why Assessing Where You Are Today Saves You Money and Makes You Safer Tomorrow

ASSESS. ADDRESS. SUCCESS.

thirty nine cyber 39

Introduction

Cyber security has become one of the most heavily funded areas of organisational investment, yet many businesses remain uncertain whether this investment is making them more secure.

The uncomfortable truth is that money spent does not always translate into risk reduced. In many cases, new tools add complexity rather than clarity, and compliance is treated as an end rather than a foundation for resilience.

This white paper explores an alternative perspective: cyber maturity. Instead of focusing solely on technologies or audits, maturity considers how people, processes, and technology work together to protect the business in practice. It reframes security as a journey of progression rather than a checklist of controls.

Across the following sections we examine why traditional spending often fails to deliver, what cyber maturity really means, and why alignment with your business model is critical. We highlight the tangible benefits that maturity assessments provide, from improved resilience and cost-effectiveness to board confidence and customer trust. Case examples illustrate where investment can be misdirected, while further sections consider cultural impact, the importance of continuous improvement, and the need to tailor assessments to the unique pressures of each organisation.

The aim is straightforward. By the end of this paper, you will have a clear understanding of why assessing cyber maturity is not simply a compliance exercise but a strategic discipline. It shows where to focus, how to spend more effectively, and how to build security that is not only stronger, but smarter and more sustainable.

Are we approaching cyber risk in the right way?

Organisations are spending more on cyber security every year, yet the uncomfortable question lingers. Is this money genuinely making us more secure, or are we simply creating more complexity, more confusion, and sometimes even more risk?

Many organisations are investing more yet still experiencing breaches

43%
businesses insured

43% - 74%
businesses breached (dependent on size)

Cyber maturity offers a way to answer this question. Instead of asking whether tools are installed, it looks at how people, processes, and technology come together to protect the business. A company may purchase an impressive endpoint detection system, but if there is no incident response process, no staff awareness training, and no clarity on who answers the phone at three in the morning, then the value of that system drops dramatically.

This issue, often described as tool sprawl, has been flagged by both academic research and government guidance. The UK's National Cyber Security Centre reminds us that security should be viewed as a capability, not a shopping list. It is a polite way of saying that just buying more does not mean doing better.

A Barracuda/Vanson Bourne study reveals that 65 % of organisations feel they have too many security tools, and over half (53 %) say the tools can't be integrated, undermining threat detection and response.

A maturity assessment is not about catching you out or marking homework, it is about showing you how well your organisation can respond to threats and therefore, risk. It tests whether money is being spent in the right areas, whether people know what to do, and whether leadership can prove resilience when questioned by regulators or customers.

Cyber threats remain common

7.78
Million incidents

21.3
Thousand per day

27%
hit rate (1.5m firms)

In short, it reframes security. Instead of asking "have we bought enough?" the more useful question becomes "are we resilient, efficient, and cost effective in the way we manage risk?" That is a far better conversation to have with your board than explaining why you bought another shiny product that nobody has the time to use properly.

Multi-vendor complexity hampers effectiveness

74% use multi-vendor stacks; 36% say complexity affects threat response

Excessive security not effective security

Here is the paradox. Organisations are spending billions on cyber security, yet breaches keep climbing. UK government research showed that businesses spent an estimated £7 billion on security in 2023, yet four in ten still reported an incident that year.

The problem is rarely lack of investment; it is misdirected investment. Boards and IT leads under pressure often approve another technology purchase because it feels like action. Firewalls, monitoring platforms, threat intelligence feeds, all useful in the right place. But stack too many together without a clear plan and you end up with tool sprawl, a confusing mess of overlapping systems that generate alerts faster than your team can possibly read them. Important risks are buried, costs spiral, and the business is no safer.

IT Admin Challenges

In the UK, 76% of IT admins prefer a single tool, yet many are burdened with multiple systems, ***48% manage 3–7 tools, 38% deal with 8 or more***

Academic studies call this security through accumulation. It sounds impressive, but the reality is less flattering. An IT manager with three different dashboards is not more empowered, they are more distracted. A firm with six scanning tools and no coherent patching process is not more resilient, it is just paying more to stay vulnerable in new and creative ways.

The humour is uncomfortably close to the truth. Some organisations are running cyber security like a gym membership. They spend every month, the equipment looks impressive, but nobody is using it properly. The investment exists on paper, but the outcomes are negligible.

This is where a maturity assessment changes the conversation. Instead of asking "what else should we buy?" it forces the better question, "what is working, and how well?" It shows you which areas need genuine investment, and which areas can be improved by simply using what you already have. In other words, less spending for the sake of it, more value for the organisation.

As my grandmother used to say: look before you leap!

Cyber maturity is one of those phrases that gets thrown around in conferences and board packs, but often without explanation. At its heart, it is not about technology at all, it is about how consistently and effectively your organisation manages risk. It is the difference between having security measures on paper and having security measures that work when tested.

Think of it like learning to drive. At the start, you may know where the pedals are, but that does not make you road safe. Over time you learn how to anticipate, how to respond in different conditions, and eventually how to drive without thinking about every single gear change. That progression from basic awareness to instinctive, embedded behaviour is essentially what a maturity model tries to measure.

A cyber maturity assessment works in the same way. It looks at where your organisation currently sits on the journey, from the basics of policy writing and patching through to advanced practices such as proactive monitoring and board-level governance. It is not about assigning blame, it is about asking whether the organisation is doing the right things, at the right level, with the right level of consistency.

Here is where it becomes interesting. Many firms assume they are more mature than they really are. They may have invested in technical controls, but when you ask the IT manager when the last incident response exercise was run, the answer is often a nervous laugh followed by silence. This is not unusual, and it does not mean the organisation is careless, it simply highlights that security is often stronger in some areas than in others. A maturity assessment shows you the whole picture, not just the parts you happen to be good at.

Imagine a business proudly pointing to its new security operations dashboard while ignoring the fact that the default passwords on its cloud services have never been changed. That is like fitting CCTV cameras around your house but leaving the front door propped open with a brick. You have invested, but you have not actually improved your security.

Only around half of medium-sized and large UK organisations report having a formal cyber security strategy

58%	66%	58%
Medium businesses	Large businesses	High income charity

This is why maturity matters. It is not about perfection; it is about progression. An organisation that understands its level of maturity can make better decisions, direct resources more effectively, and avoid wasting money on controls that look impressive but do little to reduce real-world risk.

ASSESS. ADDRESS. SUCCESS.

Ensure the approach you adopt supports your business

Once we understand what maturity is, the next question is: maturity for what? Not all organisations are built the same, and neither should their maturity assessments be. A law firm, a logistics provider, and a healthcare organisation may all pursue certification, but their risks and operations are entirely different. Assessments that ignore context risk producing recommendations that are technically correct but practically useless.

Alignment with the business model is therefore critical. Recommendations must reflect not just regulation, but how the organisation creates value, where disruption would hurt most, and what level of control is proportionate to its risk environment.

Failing to align can lead to wasted effort. Add too much bureaucracy to a lean start-up and you stifle agility. Introduce controls that clash with patient care and staff will ignore them. Even well-meaning improvements fail if they do not account for the realities of the operating model.

A better way is to treat maturity like athletic training. Every athlete needs fitness, but a sprinter, a rower, and a marathon runner cannot all train the same way. Each programme must reflect the event being run. Cyber maturity is no different. The framework remains, but the path is tailored to the business.

And this context matters, because the benefits of maturity are only meaningful if they apply to your organisation, not to some abstract model. Which brings us to the next question:

What are the real benefits of assessing cyber maturity?

If you ask most organisations why they spend on cyber security, the answers tend to fall into three categories. One, because regulators expect it. Two, because customers demand it. Three, because everyone is slightly terrified of being tomorrow's headline. These are fair reasons, but they are defensive reasons. They explain why money gets spent, not whether it is being spent well.

This is where maturity assessments prove their worth. They do not just tell you whether you have a particular control in place, they tell you how effectively that control is working, how consistently it is applied, and whether it reduces your risk. The benefits are immediate and practical.

Clarity	*A structured view of where strengths exist and where the real gaps lie.*
Value	*Directing money to deliver the greatest risk reduction rather than those that simply look impressive..*
Resilience	*Testing whether people and processes can respond effectively, not just whether a policy exists..*
Confidence	*Translating technical assessments into a language that executives can use to make informed decisions..*
Trust	*Demonstrating maturity as a differentiator, proving that the organisation can be relied upon..*

And yes, there is a hidden bonus. Maturity assessments make cyber security more human. They reduce anxiety, provide staff with clarity, and replace long checklists with achievable roadmaps. If you want to see an operations manager smile, show them a plan that makes sense.

ASSESS. ADDRESS. SUCCESS.

Making the right decision in a world of decisions is not easy

Consider the example of a mid-sized professional services firm that believed its next logical step in cyber security was to procure a security operations centre. The idea had appeal. A SOC carries an aura of sophistication, offering continuous monitoring and rapid response, and it appeared to match what peer organisations were adopting.

Yet closer examination raised questions. The firm had irregular patching processes, weak access controls, and no history of structured incident response exercises. In that context, a SOC risked being less of a solution and more of a distraction. Continuous monitoring is of limited value if the fundamental vulnerabilities remain unaddressed.

There were alternative approaches that would likely have been more effective and offered better value. Strengthening patch management would have reduced exposure to known vulnerabilities at relatively low cost. Introducing role-based access controls and multi-factor authentication would have addressed common entry points for attackers. Running even a basic incident response exercise would have built familiarity with escalation paths, communication strategies, and decision-making under pressure — all at a fraction of the cost of a SOC.

This is not to argue that advanced monitoring has no place. For some organisations with high threat exposure, or with regulatory requirements for continuous oversight, a SOC is entirely appropriate. However, for firms that have not yet embedded core controls, it represents a misalignment of investment. The organisation is effectively attempting to operate at a high level of maturity in one area while remaining at a basic level in others.

A maturity assessment frames this misalignment clearly. It identifies where investment will deliver the greatest reduction in risk, and where ambition may be outpacing capability. The lesson is not that SOCs are unnecessary, but that their value depends on timing, context, and readiness.

The Hidden Bonus: Making Cyber Less Scary for Staff

There is pressure on your team to make the right risk decision with every key stroke

Cyber security is often discussed in terms of technology, compliance, or governance. Less attention is paid to how it feels for the staff who must live with it every day. To many, security looks like a mysterious world of rules and acronyms that disrupt workflows without ever being explained.

A maturity assessment can change this dynamic. By examining processes, communication, and culture, it highlights whether staff expectations are realistic, whether guidance is clear, and whether controls are helping rather than hindering. This improves compliance, but it also improves confidence. Staff feel that they understand what is happening and that they have a role in resilience.

CISO Challenges

79% of UK cybersecurity professionals report mental health impacts from rising threats, budget constraints, and regulatory pressure

Take incident response as an example. A team that has never rehearsed an incident will see it as a terrifying unknown. Run a tabletop exercise, however, and what was once confusion becomes rehearsed familiarity. People may not enjoy the scenario, but at least they know the choreography.

The same applies to everyday practices. Password rules that make no sense, or training that feels irrelevant, create resentment and encourage shortcuts. A maturity assessment exposes these gaps and allows for more practical, human-centred improvements.

69% of employees say they would be willing to bypass cybersecurity guidance if it helped them or their teams.

Expecting employees to absorb incomprehensible security policies without explanation is like handing them the complete works of Shakespeare and expecting a polished stage performance by Friday.

No wonder shortcuts appear. By focusing on clarity, maturity assessments make security feel less like punishment and more like a shared responsibility.

You cannot fix your cyber issues with technology alone; you need to consider how your humans will behave

ASSESS. ADDRESS. SUCCESS.

thirty nine cyber 39

Threat changes, this is an arms race, so review your defensive posture continuously

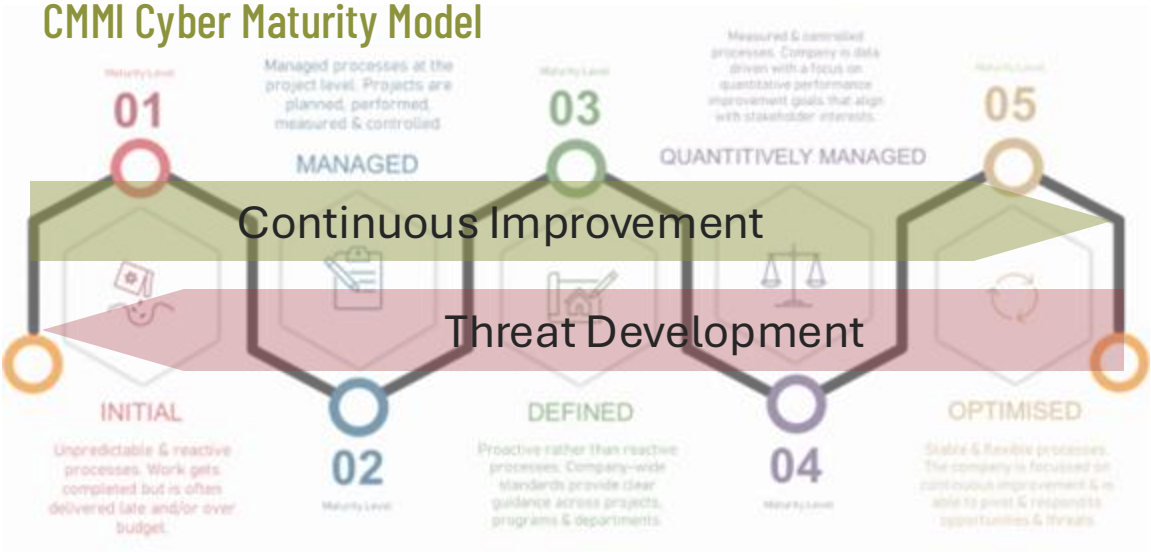
Cyber maturity is sometimes mistaken for a project with a defined end point. An organisation runs an assessment, produces a report, and ticks the box marked "secure." Cyber maturity is closer to physical fitness. You can attend the gym intensively for three months and see results, but if you stop altogether, those gains are soon lost.

Threats evolve, technologies age, staff change, and regulators introduce new requirements. A maturity assessment provides a snapshot of how well prepared you are today, but without a process for continuous improvement, that snapshot ages quickly. What felt like a strong position last year may look dangerously exposed today.

The principle of continuous improvement is well established elsewhere. Manufacturers refine processes, auditors review annually, and quality standards demand reassessment. Cyber security is no different. The aim is not perfection; it is consistent progress.

Declaring your organisation mature after a single assessment is like declaring yourself fluent in French after one weekend in Paris. You may know a few useful phrases, but the first time someone speaks quickly, you will discover your limits. Maturity is proven over time, not claimed once.

The answer lies in repetition. Regular reassessments, progress monitoring, and updated roadmaps turn a static snapshot into a dynamic capability. Continuous improvement ensures that security matures alongside the business and remains relevant as threats evolve.



Conclusion – Measure, Improve, Repeat

Act to reduce risk continuously, proportionately & inline with risk appetite

Cyber security is not won by the organisation with the longest list of tools, nor by those who pass an audit once. It is built by developing maturity step by step in a way that reflects the business being run and the risks faced.

A maturity assessment provides clarity. It shows where investment is working, where gaps remain, and how improvements can be prioritised. It offers language that boards can use, roadmaps that IT teams can follow, and evidence that customers and regulators can trust.

The lesson is simple. Maturity is not an end state; it is a process. It must be measured, improved, and repeated. This approach turns cyber security from a guessing game into a measurable capability, ensuring progress is visible, resources are well spent, and resilience becomes part of the organisation's fabric.

Measure where you are. Improve where it matters. Repeat the process. That is the discipline of cyber maturity, and it is how organisations build trust, reduce risk & waste, and prepare for the future.

In Summary

This white paper argues that cyber security spending alone does not guarantee resilience. Many UK organisations are investing heavily in tools, yet breaches and disruptions continue to rise. The problem is often misdirected investment, with overlapping systems and poorly integrated controls creating more complexity rather than reducing risk.

The concept of cyber maturity offers a better approach. Maturity assessments examine how people, processes, and technology work together in practice, not just whether individual controls are present. They show how consistently security measures are applied, whether they align with business goals, and where improvements will make the greatest impact.

The conclusion is simple but powerful: cyber maturity reframes security from being a reactive cost into a foundation for resilience, trust, and growth. Organisations that measure their maturity, improve where it matters, and repeat the process will spend more effectively, build confidence with stakeholders, and be better prepared for future threats.

thirty nine cyber 39

info@thirtyninecyber.com

ASSESS. ADDRESS. SUCCESS.