VELES

25 Questions to Reveal Your Hidden Cyber Risks in Under 5 Minutes

Executive Cyber Exposure Scorecard

A practical self-assessment for executives responsible for cyber risk, governance and operational resilience

Why This Scorecard Exists

The Executive Cyber Exposure Scorecard helps organisations identify vulnerabilities, **critical assets** and **remediation gaps** that quietly increase cyber exposure.

This assessment evaluates five executive capabilities that consistently determine how quickly organisations identify, prioritise and respond to cyber risk.

Instead of relying on fragmented reports, you'll gain a clearer understanding of where cyber exposure exists, where it is increasing and where action is needed most. The result is greater confidence for security teams, clearer visibility for leadership and fewer opportunities for hidden exposure to compound unnoticed.

How To Use This Scorecard

Rate each statement based on your organisation's current practices, not its intended future state.

There are no right or wrong answers.

The goal is to identify potential gaps in executive visibility, ownership and cyber risk governance.

Use the scale below for every statement.

RATING	MEANING	SCORE
Never	Practice not in place	0
Rarely	Inconsistent	1
Sometimes	Partially implemented	2
Usually	Mostly consistent	3
Always	Fully embedded	4

Visibility

Visibility is about knowing what matters. It measures whether leadership has a clear, current understanding of the organisation's cyber exposure, critical assets and hidden risks before they become business problems.

STATEMENT	NEVER	RARELY	SOMETIMES	USUALLY	ALWAYS
I can identify the organisation's most critical internet-facing assets					
I have visibility into unknown systems that are identified and investigated					
The cyber reporting I receive highlights business impact rather than technical severity					
The executive dashboards I rely on reflect current exposure rather than activity alone					
I understand what is not being measured					

Ownership

Ownership measures accountability. It assesses whether cyber risks have clear business owners, whether remediation responsibilities are understood, and whether issues remain visible until they are fully resolved.

STATEMENT	NEVER	RARELY	SOMETIMES	USUALLY	ALWAYS
I know who is accountable for every critical vulnerability					
I know when accountability of cyber risks changes					
I have visibility into approved exceptions to remediation					
I am informed when critical remediation activities become overdue					
I have confidence that accountability continues until remediation is verified					

Prioritisation

Prioritisation measures how effectively cyber risk is ranked and addressed. Rather than treating every vulnerability equally, it examines whether decisions are based on business impact, operational importance, and real-world exposure.

STATEMENT	NEVER	RARELY	SOMETIMES	USUALLY	ALWAYS
I understand why certain cyber risks are prioritised over others					
I have confidence that critical systems receive remediation first					
I know that security investments are reducing our highest exposures					
I understand why accepted risks remain unresolved					
I know that business impact influences remediation decisions					

Governance & Reporting

Governance & Reporting measures the quality of executive oversight. It assesses whether leadership receives meaningful information that supports decision-making, rather than simply reporting technical activity or compliance metrics.

STATEMENT	NEVER	RARELY	SOMETIMES	USUALLY	ALWAYS
I receive meaningful updates about cyber risk					
The reports I receive explain trends rather than isolated metrics					
I can clearly explain our current cyber priorities					
I am confident business stakeholders are involved in cyber risk decisions					
The reporting I receive enables better business decisions, not just compliance reporting					

Operational Readiness

Operational Readiness measures the organisation's ability to respond when a cyber incident occurs. It evaluates whether leadership, critical suppliers, recovery plans, and decision-making processes are prepared before a crisis happens.

STATEMENT	NEVER	RARELY	SOMETIMES	USUALLY	ALWAYS
I know who leads the organisation during a cyber incident					
I know that critical suppliers are included in our cyber planning					
I have confidence that recovery priorities are clearly documented					
I know our organisation has rehearsed major cyber incidents					
I understand the operational dependencies that would affect recovery					

What Your Scores Mean: Visibility

After calculating your scores for each assessment area, use the guidance below to interpret the results.

17-20

🟩 Strong Visibility

Leadership appears to have mature visibility into cyber risk. Reporting supports informed decision-making and reflects current organisational exposure.

13-16

🟨 Developing Visibility

Leadership has visibility into many important areas, but it is not yet consistent. Some decisions may still rely on incomplete reporting or assumptions.

9-12

🟧 Limited Visibility

Visibility exists in some areas, but important gaps remain. Leadership may not have a complete understanding of where the organisation's greatest cyber exposures exist

0-8

🟥 Critical Visibility Gap

Leadership has limited visibility into cyber exposure. Important assets, risks or reporting processes may not be consistently identified, creating potential blind spots.

What Your Scores Mean: Ownership

After calculating your scores for each assessment area, use the guidance below to interpret the results.

17-20

🟩 Strong Ownership

Accountability for cyber risk appears to be clearly defined across the organisation. Leadership has confidence that critical risks remain visible until remediation is complete.

13-16

🟨 Developing Ownership

Ownership is established for many cyber risks, but inconsistencies may exist. Some responsibilities or remediation activities may benefit from greater executive oversight.

9-12

🟧 Limited Ownership

Accountability may not be consistently assigned or maintained. Leadership could face challenges understanding who is responsible for resolving critical cyber risks.

0-8

🟥 Critical Ownership Gap

Cyber risks may lack clear accountability or sustained ownership. Without defined responsibility, remediation efforts can become delayed, fragmented or overlooked.

What Your Scores Mean: Prioritisation

After calculating your scores for each assessment area, use the guidance below to interpret the results.

17-20

🟩 Strong Prioritisation

Cyber risks appear to be prioritised according to business impact and operational importance. Leadership has confidence that resources are focused where they matter most.

13-16

🟨 Developing Prioritisation

Risk prioritisation is generally effective, although some decisions may still rely on technical severity rather than broader business impact.

9-12

🟧 Limited Prioritisation

Cyber risks may not be consistently prioritised according to organisational impact. Critical issues could compete with lower-value remediation activities.

0-8

🟥 Critical Prioritisation Gap

Leadership may have limited confidence that cyber resources are focused on the organisation's highest business risks. This can reduce the effectiveness of remediation efforts.

What Your Scores Mean: Governance & Reporting

After calculating your scores for each assessment area, use the guidance below to interpret the results.

17-20

🟩 Strong Governance & Reporting

Leadership receives meaningful, decision-focused reporting that supports effective oversight of cyber risk and organisational exposure.

13-16

🟨 Developing Governance & Reporting

Executive reporting provides useful visibility into cyber risk, although opportunities remain to improve consistency, business context or decision support.

9-12

🟧 Limited Governance & Reporting

Reporting may focus more on technical activity than business impact. Leadership could lack the information needed to make fully informed cyber risk decisions.

0-8

🟥 Critical Governance & Reporting Gap

Executive reporting may not provide sufficient visibility into cyber exposure. Important decisions could be made without a complete understanding of organisational risk.

What Your Scores Mean:
Operational Readiness

After calculating your scores for each assessment area, use the guidance below to interpret the results.

17-20

🟩 Strong Operational Readiness

Leadership appears well prepared to coordinate and respond during a cyber incident. Roles, recovery priorities and operational dependencies are clearly understood.

13-16

🟨 Developing Operational Readiness

Core incident response capabilities are established, although opportunities remain to strengthen preparedness, recovery planning or executive coordination.

9-12

🟧 Limited Operational Readiness

Operational readiness may be inconsistent. Leadership could experience delays or uncertainty when responding to significant cyber incidents.

0-8

🟥 Critical Operational Readiness Gap

The organisation may not be adequately prepared to manage or recover from a major cyber incident. Leadership should review response plans, recovery priorities and governance arrangements.

Scoring System: Assessment Area

Assessment Area	Your Score
Visibility	____ /20
Ownership	____ /20
Prioritisation	____ /20
Governance & Reporting	____ /20
Operational Readiness	____ /20
Overall	**____ /100**

Overall Scoring System

85-100

🟨 **Executive Cyber Exposure Maturity is Strong**

Leadership appears to have mature visibility into cyber risk. Continue validating reporting reflects operational reality and adapts to changing threats.

65–84

🟧 **Developing Executive Cyber Maturity**

Many governance practices are established, but gaps may still exist in ownership, prioritisation or executive reporting. Review lower-scoring sections to identify where additional oversight is needed.

Below 65

🟥 **Hidden Executive Exposure May Exist**

Your organisation may have limited visibility into how cyber risks are identified, prioritised and governed. This does not necessarily indicate weak technical security, but it may suggest leadership is making decisions without the full exposure picture.

Your score highlights where leadership visibility may be limited.

If this assessment highlighted potential blind spots, the next step is understanding **where** they exist.

Our **Executive Exposure Gap Review** provides an independent view of your organisation's cyber exposure, helping leadership identify hidden risks, validate current assumptions and prioritise what matters most.

Schedule an Executive Exposure Gap Review
info@velesgroup.co