9 Questions the CEO Should Ask the CISO

Not knowing what cybersecurity is doing could cost you your business. These questions protect it.



viLogics

By:Wil Klusovsky, CRO - viLogics

1 Investment & ROI

How are we deciding where to invest more or spend less on cybersecurity

✅ **Answer You Want to Hear:**

We base investments on a clear risk strategy tied to business objectives. We prioritize high-impact areas and regularly review whether our spending is reducing our biggest risks.

⚠️ **If Not:**

Push for a risk-based framework. Ask them to map security investments to top business risks, not just tools or compliance checklists.

2 Managing & Priorities

How are we prioritizing and tracking the things we need to improve?

✅ **Answer You Want to Hear:**

We maintain a living roadmap. In the next 12 months we're prioritizing <current need> and over the next 1–3 years we're building toward <desired goal>. We measure and adjust quarterly.

⚠️ **If Not:**

Require a roadmap immediately. Without a plan, investments are reactive, not strategic. This can be started with a framework assessment.

3 Biggest Risk

What is the biggest risk to our business today, and how are we addressing it?

✅ **Answer You Want to Hear:**

Right now our biggest risk is ___. Here's what we're doing, and here's the timeline to reduce that risk.

⚠️ **If Not:**

Insist on clarity. Risks should be explained in business terms (e.g., downtime, revenue loss, reputational damage), not just technical jargon.

Start with a risk assessment, record the findings, and rank risks by their likely business impact.

4 Blind Spots

What don’t we know that we should know, and how do we find out?

✅ **Answer You Want to Hear:**

We know we lack visibility in X area, so we’re testing/assessing/monitoring to close that gap.

⚠️ **If Not:**

Require ongoing threat assessments, pentesting and attack surface reviews.

Audit the existing risk register and compliance requirements for risks to the business. Don’t forget Legal.

5 Accepted v Unknown

Which risks are we accepting knowingly, and which are we accepting without realizing it?

✅ **Answer You Want to Hear:**

We’ve documented risks A, B, C and consciously accepted / transferred them.

Here are the risks we still need to assess, along with our plan to review them."

⚠️ **If Not:**

Insist on a risk register. Decisions to “accept” risk must be visible to leadership, and that decision is made by the business/asset, owner not cybersecurity or IT.

Good CEOs don't ask for reassurance.

They ask for evidence, priorities, and trade-offs.

viLogics

6 Business Resilience

How quickly could we restore critical operations if an incident disrupts them, and how do we know the plan will work?

✅ **Answer You Want to Hear:**

We can restore critical operations in X hours/days. We've defined critical systems in our business impact analysis (BIA) so we know what is priority.

We test this regularly, and here's the proof.

⚠️ **If Not:**

Demand a tabletop exercise or simulated incident. If the plan hasn't been tested, assume it won't work. A BIA is required to prioritize systems.

A full disaster recovery and business continuity plan is likely required. Those plans should be tested regularly as well.

7 Third-Party Risk

How are we protecting ourselves from partner risks and protecting our partners from us?

✅ **Answer You Want to Hear:**

We tier vendors by risk, assess them regularly, and enforce requirements. We can also provide proof of our own controls to clients & partners.

⚠️ **If Not:**

Require a third party risk management (TPRM) program and a clear process for client trust (certifications, attestation, audits).

8 Client & Investor Scrutiny

What would our key clients or investors want to know about our cybersecurity if they were in the room right now?

✅ **Answer You Want to Hear:**

They'd want assurance that we protect their data, know our risks, and have reasonable controls and processes in place for prevention and resilience. We can show that today.

⚠️ **If Not:**

Push for a business-aligned security narrative, ex: executive summary slides, client FAQs, or a one-pager for investors. Compliance certifications can be a play here as well.

9 Future Threats

What new threats or technologies could disrupt us in the next 12–18 months?

✅ **Answer You Want to Hear:**

We’re tracking threats like ___ (AI-driven phishing, deepfakes, supply chain exploits).
Here’s our plan to adapt.
It’s on our roadmap and built into budget planning for next quarter/the next fiscal year.

⚠️ **If Not:**

Require horizon planning. Ask how future threats are being built into the security roadmap and budget.

Have business leaders talk with security about what they’re planning for the future

Can your leadership team confidently answer all nine questions?

If the answers are unclear, your business may have risks, gaps, or responsibilities nobody is fully managing.

At viLogics, we build and manage cybersecurity programs around business risk, with clear priorities, accountability, and measurable outcomes.

Want to know if your cybersecurity program is delivering what your business needs?

Start the conversation with viLogics

Wil Klusovsky, CISSP, CISM, CDPSE
CRO - viLogics

