SecurityScorecard

TOP 10
Security Questions Board Members Ask

QUESTION #1

Is security a business enabler or a roadblock to production?

52% of board members reported making significant progress in improving customer trust in the past three years as a result of strengthened cybersecurity practices.[1]

To ensure your board is part of this 52% it is critical to:

- Present easy-to-understand metrics
- Identify opportunities to use cybersecurity as a market differentiator and business driver
- Partner with other executives to tie security to their KPIs and metrics reported to the board
  - Chief Risk Officer
  - General Counsel/Chief Legal Officer
  - Chief Information Officer
  - Chief Technology Officer
  - Chief Trust Officer
  - Chief Privacy Officer

QUESTION #2

What do we need to implement to get the cyber insurance coverage we need?

Obtaining insurance isn't as easy as it used to be. The requirements for insurance have become more stringent and companies could face higher premiums and less coverage, or risk not being offered insurance at all if they don't have a strong security posture.

Given these market conditions, it's important to know the basic requirements to secure insurance.

- Implementation of Endpoint Detection and Response (EDR)
- Indication of firewall usage and effectiveness
- Encryption and regular back-up of business data
- Secure provisioning process for user access rights and permissions
- Multifactor identification installed on critical systems

With these very basic elements in place and measured, organizations can work with insurance companies to ensure they are protected against losses resulting from a cyber attack.

In 2021, cyber insurance pricing in the U.S. increased an average of 96% year-over-year.[2]

QUESTION #3

Are we spending money in the right places?

Most security budgets are informed by intuition and are defined in silos away from the business. To answer this question, security teams should be able to describe cyber risk in monetary values so that all investments are justifiable and aligned with broader business goals.

Security teams need to:

- Tie specific issues to financial impact with contextualized output
- Map risk scores to current threat landscape
- Describe security performance in the form of:
    - The financial losses that could result from an incident
    - The likelihood of a breach
    - How often an incident could occur
    - How capital would be spent post-incident
    - How investments reduce expected financial losses

of IT decision makers claim their business would be willing to compromise on cybersecurity in favor of other business risks.[3]

QUESTION #4

Have we reduced our risk?

Creating a baseline and continually measuring against it is critical to ensuring security and the effectiveness of security spend.

Security teams should not only measure progress, but also communicate what that progress means in terms of risk impact. Leveraging a security rating tool can help you easily quantify your risk reduction and communicate to the board in an easy-to-understand way.

Score Impact	Risk Impact
F → D	22% reduction
F → C	40% reduction
F → B	66% reduction
F → A	87% reduction
D → C	28% reduction
D → B	57% reduction
D → A	83% reduction
C → B	40% reduction
C → A	77% reduction
B → A	62% reduction

QUESTION #5

Do we have visibility into our supply chain risk?

Your security posture is never just your security posture. A combination of yours, your vendors', and their vendors' makes up the ecosystem of organizational risk.

To build a scalable and sustainable business ecosystem risk (often referred to as third-party risk) program:

- Identify your known and unknown vendors
- Analyze risk for each vendor
- Prioritize vendors based on risk impact to your business
- Monitor continuously to stay on top of any notable issues

59% of enterprise leaders want more centralized control over their third-party relationships.[4]

QUESTION #6

What level of automation do we have in our security practice?

The average security team uses 47+ different products, yet only 39% said they are getting full value from their security investments.[5]

Automation and integration can drive improved utilization and effectiveness of existing tools.

- Integrate your SIEM, GRC, VRM, Risk Intelligence via APIs
- Elevate the most important alerts, cut down the noise
- Conduct continuous third-party management with automated vendor detection and vendor questionnaires, remove manual effort involved in point-in-time assessments

QUESTION #7

How long does it take for us to pass our customers' onboarding security processes?

A robust third-party monitoring program results in:

83% less time onboarding new vendors

83% less time on compliance validation[6]

Risk assessments of partners and evaluations of a firm's own security posture require virtually real-time analytics. Boards should have a broad understanding of the tool sets that enable close to real-time due diligence.

QUESTION #8

Do we have the right staff?

Fully staffing security teams with qualified individuals will continue to be a challenge. For teams to do more with less, they need tools that can:

- Prioritize alerts, cutting down on the noise
- Automate report development for stakeholders (including the board)
- Speed vendor on-boarding
- Improve third-party risk management
- Automatically detect "hidden" vendors

There are

600,000+

cybersecurity vacancies in the U.S.[7]

QUESTION #9

How do we get the right skills onto our team?

IT staff wear many hats and often don't have the time to take full advantage of security investments or ramp up their education to sharpen their edge with the latest innovations.

Augment your team's capacity through professional services plus ongoing security training and education to optimize and retain your existing resources, ultimately driving more business value.

87%

of businesses need skilled IT security personnel, **yet IT budgets grew only 4%.**[8]

70%

of board directors reported viewing cybersecurity as **"a strategic, enterprise risk."**[9]

QUESTION #10

If we need to make a shift in business strategy, can security keep up?

Organizations need to view each major new digital transformation initiative through the lens of cyber risk.

- Scenario planning allows leaders to consider potential gains and losses relative to other business priorities and obligations
- Embed cybersecurity into operations by making security a responsibility within every department. Solutions that provide a granular, dashboard view into systems that matter to each operational team empower non-security teams to track vulnerabilities within their systems — spreading security responsibility and management across the organization.

Tens of thousands of customers trust SecurityScorecard's risk intelligence platform to make faster and smarter business decisions and communicate those decisions across all levels of stakeholders.

Create your FREE account today, and enable your security teams to stay ahead of important security strategy questions.

GET STARTED

1. Survey of more than 400 global companies, weforum and PwC, 2020
2. How to find ransomware cyber insurance coverage in 2022, TechTarget, 2022
3. Business Friction is Exposing Organizations to Cyber Threats, TrendMicro, 2022
4. A crisis in third-party remote access security, SecureLink and Ponemon Institute, 2021
5. 53% of enterprises have no idea if their security tools are working, Help Net Security, 2019
6. The Total Economic Impact™ of SecurityScorecard, Forrester, 2021
7. What's the Latest on Cyber Talent and Staffing Shortages?, Security Boulevard, 2022
8. Unit 42 Ransomware Threat Report, Palo Alto Networks, 2021
9. 2020–2021 NACD Trends and Priorities of the American Boardroom, NACD, 2021

SecurityScorecard
The Power of Knowing

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1701
International: +1(646) 809-2166