



MOVING TO RISK-BASED CYBERSECURITY

The old way of measuring cybersecurity success isn't working.

CIOs and CISOs at enterprises large and small struggle with similar challenges:

The potential attack surface is widened by problems like unregistered public IPs.

"We're swamped by tools & data."

The average enterprise has **16+ security tools**. 12% of organizations have **46+ tools**

"Our teams have limited visibility."



"Manual processes can't keep up."

A lack of cybersecurity automation compounds the IT Security skills gap.

Cyber Risk is Now a Board-level Concern

Cybersecurity risk is now a regular topic in the boardroom. Security leaders should simplify how they discuss cyber risk with executives by defining it in terms of bottom-line business risk.

1
2
3

+50%

Quarterly board meeting agendas include the CISO



\$4.24M

Average cost of a data breach, 2021



800

Avg. mentions of cybersecurity in quarterly earnings reports



Don't Count Vulnerabilities, Count Risks!

The old way of counting vulnerabilities to measure cyber risk is ineffective. While the total number of vulnerabilities is soaring, just a small subset pose material risk.

185,446

100%

Universe of all known vulnerabilities

55,186

29%

with exploit available

Pose Greatest Risk

3,854

2%

with exploit code weaponized

718

.38%

exploited by malware

307

.16%

exploited by threat actors

177

.095%

named vulnerabilities (Log4Shell, Heartbleed)

Follow this 3-Step Cyber Risk Process...

Qualys suggests a three-step cyber risk management cycle that continuously monitors the threat landscape, enables quick response, and measures the metrics that company leadership cares about.

1



Assess Risk

Gain visibility & control over all IT assets in your environment.

- ✓ Understand your organization's total attack surface
- ✓ Inventory all assets for baseline threat assessment
- ✓ Use a security platform that can quantify business risk

2



Reduce Risk

Consolidate your security stack into a unified platform.

- ✓ Simplify the number of cybersecurity tools used by your teams
- ✓ Use automation capabilities for risk monitoring, detection, and remediation
- ✓ Assign actions to reduce risk across Security, IT, and Compliance

3



Report on Risk

Adopt automated dashboards with clear, risk-defined metrics.

- ✓ Measure risk against industry standards, peer benchmarks, and best practices
- ✓ Report on risk by need: Business metrics for executives; Technical metrics for security practitioners
- ✓ A comprehensive cybersecurity platform will automatically do both

Read More on the Qualys Security Blog:
Transitioning to a Risk-based Approach to Cybersecurity

