EXPERT PAPER

Expert Paper

How to benchmark your organization's security posture in 5 easy steps

Autobahn security

Executive summary

Are you benchmarking everything except your cybersecurity KPIs? You could be missing out on vital information.

In this expert paper, we examine how benchmarking your cybersecurity posture can benefit you by:

- Helping your organization flourish through competition
- Drive better governance through outside benchmarking
- Reduce your chance of major incidences by staying above the average via benchmarking
- Gain transparency into how well your cybersecurity budget is being spent

About Autobahn Security

Autobahn Security is a SaaS platform that saves IT security professionals time — and empowers IT teams to make their networks more secure.

Our platform aggregates, filters and prioritizes vulnerabilities from multiple scanners and turns them into easy-to-understand remediation guides.

Autobahn Security is the result of decades of white-hat hacking and security consulting experience for Fortune 500 companies. Autobahn Security is trusted by companies across multiple industries in over 20 countries, including Allianz, SwissPost and Taboola.

The myth of the all-knowing hacker

This expert paper attempts to debunk the perception that hackers are always ahead of you.

Instead, we argue that companies only need to keep themselves *relatively* protected from hackers, who are notably lazy — and chase the weakest members of the herd.

Whether or not you look attractive to bad actors depends on what other companies look like in terms of cybersecurity.

Rather than chasing perfection, organizations just need to maintain an above average level of cybersecurity protection.

However, to gauge the industry status quo, you must have benchmarks to compare against. This gives you a way to know your current standing and provides shortcuts to get cyber fit — and win the race against hackers.

Read this case study to learn how a leading software company handled 1 million security issues in just 80 easy workouts.

Read now

Why internal and external benchmarking matters

Why do internal benchmarks?

The short answer is: we want to win the friendly competition in our own company, so we are set up for the not-so-friendly battle with hackers.

The longer answer is that there are lots of benefits to internal benchmarks. With a reliable KPI for measuring your cybersecurity posture, you can ask your management team this simple question: “Which department can improve their cybersecurity in the fastest and most sustainable way?”

This internal competition can work magic: departments or subsidiaries compare themselves, share best practices and jointly address common cyber flaws. If you give them usable KPIs and and a way to track, benchmarking activities give personnel the tools they need to get serious about cybersecurity.

Why do external benchmarks?

External benchmarks provide a good overview of where you stand in the industry. Perhaps you’ve worked hard to get your Hackability from 72 to 45. But if your benchmarks are showing you’re still at the bottom of the pack, this can be a great argument to show to management to underline how you need to keep focus on the topic or perhaps increase budgets to tackle it more holistically.

Learn how having just 1 Hackability KPI can provide organizational alignment

Read now

The key 5 stages of benchmarking

1. Planning

You need to decide what to benchmark. For many organization, any benchmarking is new territory.

One key reason why many companies do not benchmark their cybersecurity KPIs is they think the global hacker threat does not concern them directly. According to a survey by Munich Re, 83% of participants estimated their own company's protection level against digital threats as insufficient. The SME segment, however, remained unimpressed: 39% of C-level respondents were not or only somewhat concerned.

Yet another reason why cybersecurity doesn't get benchmarked is the lack of awareness about reliable KPIs. These should be:

- **Accessible to any IT professionals, not only those specializing in cybersecurity**
- **Expressed from the hacker's point of view**
- **Actionable**

2. Set relevant KPIs

What are the relevant KPIs for benchmarking in cybersecurity?

Hackability Score

The Hackability Score deals with *process security*. It collects many measurements from your security scans and saves you the hassle of dealing with the raw data, which often frustrates security personnel.

This score targets your organization's ability to follow established security best practices in 3 dimensions: (1) patching, (2) hardening, and (3) exposure.

Knowing how hackable you are is useful for both internal and external benchmarking. The Hackability Score enables dialog about cyber risks and fuels the improvement race between peers in your organization. And it puts your cyber protection level in perspective by showing the target industry-standard corridor of hackability values.

Cyber Security Rating benchmarks your business among peers

This KPI adds *technology security* to the race. Your company and its peers are individually assessed and then measured and scored against a global benchmark of a diverse set of companies.

It captures whether your corporate network is easy to maintain and protect from common attacks. For example, protection from malicious emails indicates that security technology is used effectively.

This score highlights the idea that a clean technology stack facilitates security management and enables staff to become experts in leveraging security features.

3. Analyze the data

The beauty of Autobahn Security approach is that the Hackability Score and the Cyber Security Rating do the analytical work for you.

You get to see a couple of numbers and you already know where you stand as a company compared to your industry peers.

In addition, for internal benchmarking, you learn how well your departments are performing in the friendly competition towards cyber fitness.

4. Develop an action plan

The Autobahn Security platform is built on the assumption that those actions that lower hackability the most also complicate hackers' life the most. And to help you remediate efficiently by focusing on exactly those actions, there are workouts.

These are user-friendly tutorials that give your IT professionals – for example, system administrators who do not specialize in cybersecurity – simple steps to patch and harden vulnerable systems and devices and reduce their exposure. Like keeping fit by doing regular exercises, you do the workouts to become cyber fit.

The more you use your cyber muscle, the better you become at applying the recommended cybersecurity practices and improving your hackability score.

5. Monitor progress

Ongoing monitoring is also made easier if you have the correct benchmarks and KPIs set.

The Hackability Score is just one number in the range between 1 and 100 that should become lower based on your IT personnel's activities in step 4. For internal benchmarking, you only monitor how fast the score drops across your departments or subsidiaries. And if hackability gets reduced efficiently, you know that your cybersecurity budget is being spent well.

Cyber Security Rating is also quite simple: it gives you a few values to monitor — and take note of when when you see that your company's results deviate from the industry peers.

The rating scheme is very simple. The benchmarking follows a percentile scoring function to reflect the way adversaries operate by looking for the easiest target.

To illustrate, if you receive a score of B, it means that you're a 'fairly difficult' target for your adversaries. And if your score is F, it shows that your IT assets might be in real danger.

However, if your industry peers receive A while you get a B, it means that you must catch up on a few areas to avoid falling below the average protection level.

To quote from an example report:

"Company X achieved an overall Cyber Security rating of D. That puts you a little behind your peers, who have an average rating of C. You could start boosting your efforts in the area of Process Security by resolving patching and hardening issues. As for Technology Security, where you scored an A in each subcategory, you are doing better than your peers."

Expert Paper

How to get started — and what you can expect in Week 1

01. Understand your issue remediation process and pain points

02. Walk through the key aspects of the platform

03. Set up scans

04. Evaluate scan results

Request your free cyber expert consultation right now

In your individual tailored discussion, an Autobahn Security expert will evaluate your individual challenges, provide a product overview, explain our value process and discuss potential milestones and next steps.

You can also benefit from a free all-access trial of the software, with no obligation.

Talk to a member of our team to see how Autobahn Security can help make your organisation Cyber Fit

Book a free expert call