BITSIGHT®
The Standard in SECURITY RATINGS

Using Security Ratings for Cybersecurity Benchmarking

Introduction

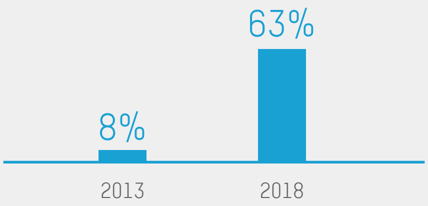
As the economy becomes more and more global, businesses are forced to stay ahead of an increasing number of competitors. The organizations that succeed will be the ones who take the time to understand their competitors, then consistently outperform them in key areas.

Benchmarking is the process of researching competitors and peers and setting internal performance goals based on that research. By examining other companies' KPIs in areas of significant importance, such as sales, profits, or productivity, then comparing those indicators to internal performance, a company can allocate resources and prioritize objectives more strategically.

Benchmarking is a well-established practice among successful organizations, but the areas these organizations choose to benchmark have not always evolved with changing business concerns.

Cybersecurity is one major area that's underrepresented in benchmarking initiatives. In a survey of almost 1,300 CEOs conducted by PWC, **63% of respondents** said they were "extremely concerned" about cyber threats in 2018, more than any other category. In 2013, just 8% of CEOs said the same.

Based on these findings, it's obvious that concerns about cyber risk are on the rise. However, many businesses continue to overlook cybersecurity when performing benchmarking exercises. Without strategic knowledge about the security of competitors and peers, these companies risk falling behind.



The share of CEOs that are extremely concerned about cyber threats is rising rapidly.

Source: PWC January 2018

In this Ebook, we'll compare and contrast available benchmarking tools, explore why cybersecurity benchmarking is so important, and detail a framework for effective cybersecurity benchmarking.

95%

of CIOs expect cybersecurity threats to increase and impact their organization.

Source: Gartner 2018

CYBERSECURITY BENCHMARKING TOOLS

More and more, business leaders are beginning to understand the realities of increasing cyber risk. They realize that every business is exposed to threats, those threats are constantly evolving, and no matter how many protections a business has in place, some are bound to slip through. According to a 2018 survey from Gartner, **95% of CIOs** said that they expect cybersecurity threats to increase and impact their organization.

Since perfect cybersecurity performance is no longer a realistic goal, businesses are forced to generate new objectives. By creating cybersecurity benchmarks and comparing them against competitors and industry peers, security leaders can set clear goals and define new security strategies.

However, benchmarking requires simple, quantitative metrics, and when it comes to quantifying cybersecurity, many companies don't know where to start. According to BRG, "[IT] leaders have difficulty assessing and communicating the effectiveness of their programs. Critically, many do not know how to even gauge the performance of their cybersecurity programs."

The problem of objectively defining cybersecurity performance is a tricky one. Because performance relies on things that don't happen (hacks, data breaches, downtime, etc.), there are very few simple metrics with which to track an organization's performance over time, or to compare against peers and competitors.

The metrics that security programs have traditionally generated, like the number of infected workstations or the number of open ports, are extremely technical. That makes them difficult to understand, compare, and communicate to others (especially leadership). These metrics also depend on internal information, rather than objective and standardized information that could be used to compare separate organizations.

The process of benchmarking an organization's security performance starts with developing common measurements of success that are easy to understand. There are a variety of techniques and tools available to help create these metrics. Let's break down a few of them:

Internal Assessments

One of the most common tools used to determine an organization's cybersecurity posture is an internal assessment. In this process, a staff member or team compares existing security controls, policies, procedures, and performance against a list of best practices. They either get their data from direct technical sources, such as running a malware scan, or by asking IT leaders to fill out questionnaires.

These assessments can be valuable, but the process of conducting them includes many opportunities for biased or incomplete information to alter results. For example, the best practices referenced might not be up-to-date or comprehensive. IT leaders might fail to enter accurate information in their questionnaires. The assessor might not even think to examine certain areas of concern.

Internal security assessments are also very time-consuming. According to a March 2018 commissioned study conducted by Forrester on behalf of BitSight, it typically takes two weeks to two months to complete a manual assessment.

Most importantly, internal assessments only provide a point-in-time view of an organization's cybersecurity posture. In order for these types of assessments to be considered effective benchmarking tools, they need to be conducted more frequently than most organizations are able to support. In the end, they still don't provide the kind of common metrics that businesses can use to have company-wide conversations about cybersecurity.

> *Internal assessments only provide a point-in-time view of an organization's cybersecurity posture.*

Third-Party Audits

Many organizations, especially those in highly-regulated industries, have their information security audited on an annual basis. These audits are similar to internal assessments, but they are conducted by external companies. This helps to remove a fair amount of bias from the assessment process, but a number of problems remain. These audits still take weeks or months to complete, the results of still only represent a single point in time, and they still only produce difficult-to-leverage information.

In addition, these audits are typically focused on keeping an organization in compliance with regulations, rather than protecting them from cyber threats. While compliance is undoubtedly important, being compliant does not make an organization secure. If a company wants to benchmark their compliance, then these audits could be extremely useful. For cybersecurity benchmarking, however, they leave a lot to be desired.

Penetration Testing

Penetration testing, or "pen testing," is the act of "hacking" your own IT targets in order to evaluate whether security controls are working, identify vulnerabilities, and make recommendations for remediation. Unlike an actual cyber attack, a pen test is conducted in a controlled way by a professional hired by the target organization, so no systems or data are really in danger.

Pen tests are extremely useful for determining whether a company's cybersecurity program is actually able to stop the attacks it was designed to prevent. While the results of these tests could be useful for benchmarking across organizational departments, they don't provide much value when comparing one organization against another.

In addition, these tests only provide specific results about the ability to withstand particular kinds of attack. To pen test a system with every possible strategy a real attacker might use would be impossible. In addition, the results still need to be translated into numbers that Board members and executives can understand.

To pen test a system with every possible strategy a real attacker might use would be impossible.

Free Security Assessment Tools

A variety of organizations and technology vendors have developed tools to help companies analyze the security of their applications, networks, or business units. Many of these tools are even available for free online.

These assessment tools take a few different forms. Some are designed to help users scan specific pieces of software for potential security risks. Others are designed to evaluate systems for compliance with vendor-agnostic best practices.

These tools can be useful for determining an organization's security posture and comparing it against internal units. However, the results of these assessments can only be used for comparison against competitors or peers if those companies voluntarily share their results, which is unlikely.

SIEMs

Security intelligence and event management (SIEM) software products give cybersecurity professionals real-time insight into security incidents. This data can be used to respond to attacks quickly, and historical logs can also be used to generate reports about where, when, and how often cyber threats are affecting an organization.

Unlike many of the other items on this list, SIEMs support the ability to continuously monitor cybersecurity performance. Whenever the time comes to start benchmarking, a user can open their SIEM dashboard and generate an up-to-date report.

However, most SIEMs only offer data about where incidents have occurred, not where they're likely to occur, making them an incomplete continuous monitoring solution. In addition, because these systems handle sensitive security information, data for benchmarking will be limited to internal companies or business units.

Security Ratings

Security ratings, like those offered by BitSight, are specifically designed to overcome the shortfalls of the other benchmarking tools mentioned in this section. In fact, they complement other solutions like internal and third-party assessments, SIEMs, and penetration testing.

Security ratings gauge the overall cybersecurity posture of an organization based on a variety of externally observable factors. The actual ratings are typically generated on a numeric scale. For BitSight, these ratings range from 250 to 900 with lower ratings **correlating to a higher likelihood of breach.**

In addition to measuring overall cybersecurity posture, security ratings can be used to measure performance in specific areas, such as botnet infections, spam propagation, patching cadence and TLS/SSL certificates.

Unlike internal and third-party manual assessments which only capture point-in-time views, security ratings offer a continuous picture of security performance. BitSight Security Ratings, for example, are updated on a daily basis. This real-time visibility into the security environment enables the most accurate benchmarking results.

Critically, unlike most of the tools we've explored so far, security ratings are outside-in. In other words, the ratings are generated by an algorithm that looks at a standardized range of factors which can be observed from the outside, and don't rely on proprietary internal information. This has two important consequences: First, security ratings are unbiased. Second, security ratings can be used to analyze any organization, not just one's own. This enables the comparison of benchmarks with competitors, best-in-class companies, global leaders, and more.

Finally, security ratings are easy to understand. With security ratings, benchmarking cybersecurity becomes simple. Measuring security becomes similar to measuring other business KPIs. The single security rating number provides an organization's overall state of cyber risk along with the ability to drill down for more in-depth analysis of individual risk vectors. Security ratings are objective, verifiable, actionable, and easy-to-report to non-technical individuals.

BENEFITS OF CYBERSECURITY BENCHMARKING

Security ratings provide the how of cybersecurity benchmarking. Now let’s discuss the why. The practice of benchmarking cybersecurity using security ratings has significant advantages for businesses that take part, including:

Quantifying Security Performance

Once a business is able to quantify their own cybersecurity performance and the performance of others, an array of analytical and operational possibilities open up. Some of these possibilities go way beyond what’s typically thought of as “benchmarking.”

With comprehensive numbers that indicate security success or failure, an organization can leverage historical data to understand how and why their security posture evolves over time in response to changing budgets, dynamic risks, rotating personnel, and other factors. These metrics can also be used to track the effectiveness of specific security initiatives.

Security ratings become the common language of security throughout the entire organization, enabling data-driven conversations among IT leaders and their colleagues. Security ratings can be used to communicate with non-IT teams, with vendors, and, importantly, with the Board and C-suite. With more digestible security metrics, executives can better understand their risk and improve decision-making.

Understanding How You Compare

In order to maximize the value of cybersecurity benchmarking efforts, organizations should strive to understand their security performance in a variety of contexts. These can be classified into a few categories:

- Best-in-Class — compare security performance against the top global performers in your industry.
- Direct Competitors — discover where your security performance falls in comparison with your closest rivals.
- Local Competitors — learn how your business stacks up against peers or competitors within a geographical boundary.
- Internal Business Units — find out how the security performance of one department or unit compares to others within your organization.
- Branch Offices — compare the security performance of branch offices operating in different locations.
- Subsidiaries — track the performance of separate companies within your organization or newly acquired companies.

A business can use benchmarking data from any of these analyses to inform decision-making and goal-setting. For example, if your cybersecurity performance is lagging behind your peers within a parent organization, you can work to meet or exceed the organizational average. Or, if your cyber security posture is better than a direct competitor, your company can leverage that as a competitive advantage in differentiating your company.

This type of comparative analysis helps CIOs, CISOs, and other IT leaders win additional resources for information security initiatives. On one hand, these leaders can use their benchmarks to prove the efficacy of cybersecurity spending. On the other, they can use the performance of competitors to spur business-focused Board members to action.

Remediating Security Issues

Security ratings provide visibility into the overall state of cybersecurity for an organization, which allows business leaders to understand how well their current security strategy is working. Importantly, BitSight Security Ratings also provide insight into a variety of risk vectors. These insights can be leveraged to quickly identify areas of weakness and build remediation plans.

CIOs and CISOs have limited resources to allocate toward a wide range of cybersecurity tools and programs. Having access to benchmarks can be invaluable in deciding where to put those resources. For example, if a majority of your competitors and industry peers have significantly better performance in one area than your company does, that's a good indicator that you need to improve. In addition, if competitors with known data breaches or other cybersecurity issues have weak performance in certain areas, beefing up remediation programs in those areas can keep your organization from becoming the next target.

> *Creating performance benchmarks by assessing a wide variety of peers, competitors, and internal units can help IT and security leaders stay on the cutting edge and stay competitive.*

With so many risks to consider as part of the cybersecurity landscape, it's not always easy to keep up with which controls and policies are considered best practices and which may be obsolete or out-of-date. Creating performance benchmarks by assessing a wide variety of peers, competitors, and internal units can help IT and security leaders stay on the cutting edge and stay competitive.

FRAMEWORK FOR EFFECTIVE CYBERSECURITY BENCHMARKING

Now that we've established the importance of security ratings for benchmarking and learned how cybersecurity benchmarking can benefit an organization, let's walk through a recommended framework for beginning the cybersecurity benchmarking process.

1. Request Your Security Ratings Snapshot

The first step in any benchmarking process is to quantify your own performance. When it comes to cybersecurity, the simplest way to do this is to request a Security Ratings Snapshot for your organization to get an initial baseline of your current security posture. You can use this rating to see how you compare to industry peers and competitors, and gain insight into areas of your security strategy that might need to be improved.

2. Understand the Security Ratings Methodology

Understanding how security ratings are determined will help you use those ratings for optimal decision-making, and help you receive buy-in for your benchmarking efforts.

3. Compare Your Rating to Previous Experience

Does your security rating mesh with your previous ideas about your organization's cybersecurity performance? If it's higher or lower than you expected, performing a gap analysis to understand why can help you reinforce preexisting assessment efforts.

4. Identify Targets for Comparison

At this stage, you can choose to compare your security performance with competitors, industry peers, best-in-class companies, internal business units, branch offices, or any of the other categories discussed in this Ebook. If you choose to compare your performance to external organizations, choose 5-10 for a good sample size.

5. Run Comparison Reports

Some security ratings platforms have reporting features that allow users to generate simple overview reports, historical reports, and more. These reports enable you to compare your current cybersecurity performance to competitors, and see how you've compared over, say, the last 12 months. You can also choose to run reports comparing performance in specific risk areas. You can run these reports on a regular basis to track changes in performance over time, then communicate those reports to executives & board members.

6. Create Action Plans

Now that you understand how your organization compares to peers and competitors, it's time to leverage that data to improve your cybersecurity strategy.

You might decide to evaluate your existing cybersecurity tools to determine their effectiveness, potentially freeing up resources that can be allocated elsewhere. You could also ask the Board for more resources, using your benchmarking reports as hard evidence of your department's needs.

In addition, you can use benchmarks to set short and long-term goals with objective measurements. For example, as a long-term goal you could aim to raise your overall security rating to a level on-par with the top-performing organizations in your industry. As a short-term goal, you could make efforts to improve your patching cadence rating to be higher than your three closest competitors.

Security ratings providers like BitSight also enable users to set up automated alerts for ratings that dip below certain thresholds. Using your benchmarking findings to inform these thresholds will help your organization keep pace with peers when it comes to mitigating cyber risk.

CONCLUSION

As cyber threats continue to increase in volume and complexity, security has to take a central role in an organization's business strategy. Businesses have long understood the importance of benchmarking for success, but have avoided benchmarking their cybersecurity performance because of a lack of easy-to-use metrics.

Security ratings are the ideal benchmarking solution for measuring cybersecurity performance. These ratings are continually updated, leverage standardized external data, are created based on a variety of risk vectors, and are simple to understand and communicate.

> *Security ratings are the ideal benchmarking solution for measuring cybersecurity performance.*

With the power of security ratings, business leaders can gain a more thorough understanding of their cyber risk and security posture as compared with a variety of peers and competitors. Then, these leaders can use that understanding to improve strategy and decision making.

There are no more excuses. Cybersecurity benchmarking isn't just a possibility — it's a necessary business practice.