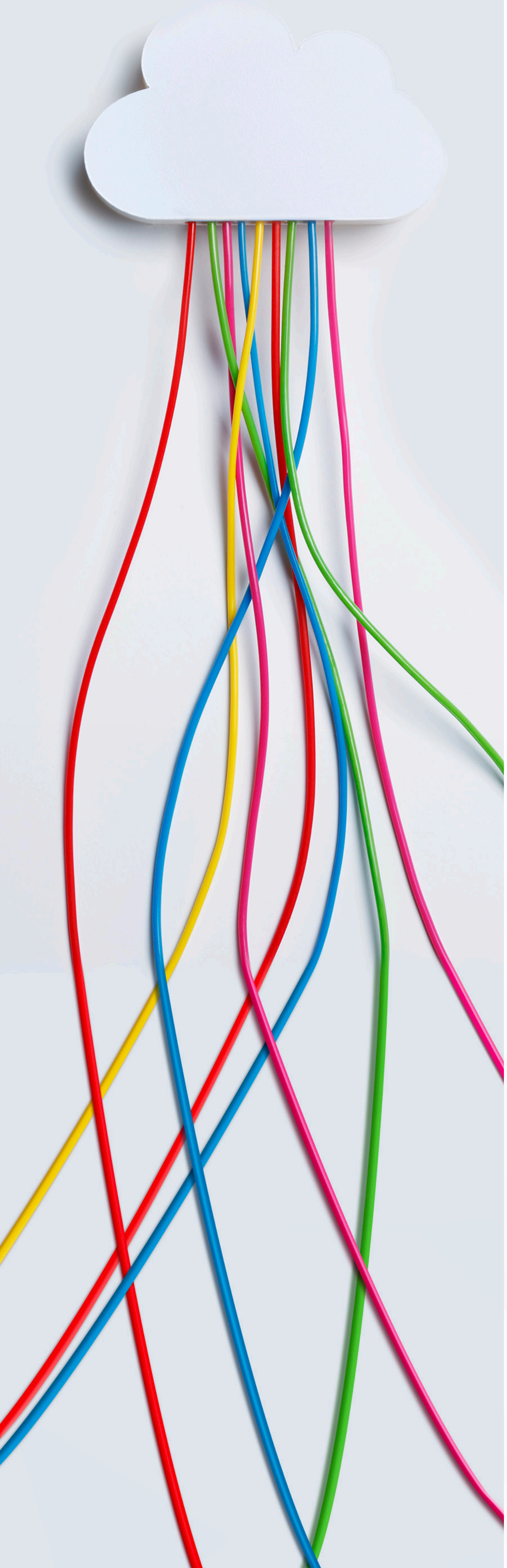
BITSIGHT®
The Standard in SECURITY RATINGS

Cybersecurity Benchmarking & Security Performance Management

A No-Guesswork Approach for CIOs



Introduction

CIOs, CISOs, and other security and risk leaders are expected to know the answers to a few simple questions:

How secure is the organization?

Are we improving over time?

Are our investments in cybersecurity paying off?

Are we more or less secure than others in our industry?

But as every cybersecurity professional knows, these questions aren't as simple as they seem. Cybersecurity's big secret — and the biggest source of anxiety for CIOs — **is that it's hard to tell what actually works**.

Audits, assessments, software tools, and “best practices” each involve a certain amount of guesswork and finger crossing. And as far as peers and competitors are concerned, who’s to say how you compare? Legacy benchmarking methods are time-consuming and **don’t always produce accurate data**.

But the Board and other executives aren’t going to stop asking these questions. They need to know the state of the organization’s cybersecurity, and they expect that information to be communicated in a way that’s easy for them to understand.

> *A new, data-driven approach is required to maintain security, minimize risk, and reduce costs.*

So the CIO is forced to make assumptions, guesses, and judgement calls, informally synthesizing what they know about their team’s performance. Otherwise, they have to spend valuable time aggregating complex metrics in an effort to quantify cyber risk, only to have **the results become outdated almost immediately**.

A NEW APPROACH

The traditional approach to security performance management described above is unsustainable in the long term. A new, data-driven approach is required to maintain security, minimize risk, and reduce costs.

Thankfully, this new approach exists, and has already been implemented by leading organizations around the world.

A key component of this data-driven approach is the security rating.

What is a security rating?

A security rating is a data-driven, dynamic, validated measurement of an organization's cybersecurity performance. These ratings are derived from objective, verifiable information, and are created by independent organizations.

Because they're independently generated and continuously updated, **security ratings take the uncertainty out of managing a cybersecurity program**. *How secure is the organization?* Well, today our rating is a 710, but last month it was a 650, so we're improving.

In other words, security ratings empower CIOs to take a risk-based, outcome-driven approach to managing cybersecurity performance through broad measurement, continuous monitoring, and detailed planning and forecasting.

The result? **Measurably reduced cyber risk**.

Security ratings are also based on externally observable, non-intrusive data; they don't rely on proprietary information from the organizations being rated. That means benchmarking becomes as simple as comparing your rating to the rating of a competitor, peer, or industry average.

Finally, security ratings act as a baseline metric of cybersecurity performance. **Think of them as the "profit margin" of cybersecurity** — one big KPI that puts all the others in context. When other executives and the Board speak the same language as the CIO or CISO, work becomes more collaborative, resource allocation becomes simpler, and it finally becomes possible to set goals that actually make sense.

In this ebook, we'll describe in detail how this no-guesswork approach can be applied to security performance management, benchmarking, and reporting. In each section, we'll provide an actionable "next steps" strategy for CIOs and other security and risk leaders to apply in order to begin the transition into this data-driven paradigm.

The No-Guesswork Approach to **Security Performance Management**

Security performance management has traditionally involved a series of judgement calls.

As discussed above, even answering a question like “are our investments in cybersecurity paying off?” becomes difficult when the only true metric of success is whether or not you’ve experienced an incident this month.

While audits and assessments can help shine some light on the situation, **they aren’t a long-term solution**. Even if we ignore the cost of these methods and their associated disruptions, we’re still left with results that reflect security performance only at a single point in time.

In other words, **unless you’re performing audits on a daily basis, you don’t have true visibility into what’s working and what isn’t.**

Unless you’re performing audits on a daily basis, you don’t have true visibility into what’s working and what isn’t.

USING SECURITY RATINGS FOR CYBERSECURITY PERFORMANCE MANAGEMENT

As objective, independent, baseline key performance indicators, security ratings are the missing piece in this puzzle.

These ratings provide critical insight into performance that gives CIOs and CISOs the ability to track progress over time, set goals, prioritize different parts of their programs, and determine the effectiveness of their investments.

> *In order to truly quantify cybersecurity, you need a metric that can act as a KPI for the entire program.*

TRACKING PROGRESS AND SETTING GOALS

Specific technical metrics like the number of ports closed, software patches made, or botnet infections in a system are too narrow to reflect security performance as a whole. Meanwhile, overall metrics like number of confirmed incidents involve too many variables (you never know when you're just getting lucky).

In order to truly quantify cybersecurity, you need a metric that can act as a KPI for the entire program. Enter security ratings.

By comparing the organization's current security rating to past performance, security leaders can accurately gauge whether or not their team's efforts are paying off.

This information can also be used to **set reasonable, actionable goals for improvement**. Instead of vague promises that carry little accountability, a CIO can motivate his team to, for example, increase the organization's security rating by 50 points in the next two months.

Don't wait to start tracking.

Some security ratings service providers offer historical data on the companies in their database, including yours. BitSight, for example, includes 12 months of historical data, so you can come out of the gate with a year's worth of progress to analyze.

Using security ratings for performance management also enables CIOs to see their cybersecurity through the eyes of key stakeholders.

Security ratings are rapidly becoming a standard method for deciding whether or not to work with vendors, integration partners, M&A targets, insurance applicants, and others — by using them internally, you can see your business the way current and future partners see your business, and resolve any issues **before they become obstacles to success.**

ALLOCATING RESOURCES

Combining information from your most recent cybersecurity audit with your organization's current security rating, you can effectively determine which parts of the program need resources *right now*.

The continuous monitoring capabilities provided by security ratings enable CIOs to prioritize like never before. For example, if your malware-fighting is above average, you can move some resources towards diligence efforts like patching and updating, or vice-versa.

By continuously monitoring the effectiveness of your resource allocation, you can avoid wasting time and money making exponentially more difficult improvements to already finely tuned controls, and instead **target low-hanging fruit you may have otherwise missed**.

> *The continuous monitoring capabilities provided by security ratings enable CIOs to prioritize like never before.*

Balancing the scales this way on a weekly or monthly basis produces a **leaner, more effective cybersecurity program** that can do more with existing resources.

DETERMINING ROI

Finally, security ratings can be used to hold cybersecurity vendors accountable for the performance of their products or services.

Did that consultant you brought in last quarter have a positive effect on the company's cybersecurity posture? Did that tool you bought to stop malware measurably improve your company's performance in that category?

Security ratings enable CIOs to answer these questions quickly and definitively. The result is a new freedom to dispense with software, services, or personnel that aren't actively contributing to real improvement.

Next Steps:

1. *Research and choose a security ratings service provider.*

2. *Using historical security rating data, see if you can find a correlation between changes to your rating and changes made to the cybersecurity program.*

3. *Take a deep dive into your rating to see if any specific risk vectors should be prioritized for improvement.*

4. *Set a goal for improving your security rating by a set value in a set time frame.*

The No-Guesswork Approach to Cybersecurity Benchmarking

In order to understand how much to invest in cybersecurity and in what areas, you need a benchmark. In order to set a benchmark, you need to determine how your organization compares to peers and competitors.

There are two methods traditionally used for cybersecurity benchmarking:

Formal benchmarking involves gathering data on peers and competitors, analyzing that data, and using it to create benchmarks. This can be done in-house or through a third party.

Most formal benchmarking activities only provide insights for a **particular point in time**. Peers and competitors are constantly changing, and those changes can cause major fluctuations in cybersecurity posture. These analyses are also expensive, time-consuming, and rely on subjectivity to fill in the blanks when proper data isn't available.

Informal benchmarking doesn't necessarily involve hard data. For example, a CIO may be a part of an online forum or group that meets monthly to discuss cybersecurity.

Informal benchmarking doesn't produce exact results. It's one thing to know that a peer is investing heavily in user security awareness training — it's another to know if that training is actually working.

And of course, some organizations won't be interested in sharing their cybersecurity practices. Participants in these types of forums must also consider antitrust issues and other legalities.

> *It's one thing to know that a peer is investing heavily in user security awareness training — it's another to know if that training is actually working.*

USING SECURITY RATINGS FOR DATA-DRIVEN BENCHMARKING

BitSight, a leading security ratings service provider, has over 140,000 organizations in its rating database. In the time it takes to formally assess one competitor the old way, one could compare their own organization to **hundreds or thousands of competitors and peers**, or simply use provided industry averages.

For peers and competitors of particular interest, you can dive deeper into the data. Using the BitSight platform, you can examine more than 20 specific risk vectors for each rated organization, including your own. These risk vectors span four categories, including **compromised systems** (what's already been affected?), **diligence** (which systems have a higher likelihood of being compromised?), **breach events**, and **user behavior**.

This level of granularity gives CIOs the visibility they need to set benchmarks and allocate resources to areas where they may have fallen behind.

What's in a security rating?

BitSight Security Ratings include granular data on a variety of risk vectors, including:

» Botnet infections
» Potentially exploited machines
» Spam propagation
» Unsolicited communications
» Malware servers
» Open ports
» Web application headers
» Patching cadence
» Insecure systems
» TLS/SSL certificates
» TLS/SSL configuration
» Sender policy framework
» Server software
» DomainKeys identified mail
» Desktop and mobile software
» File sharing

When you combine security ratings with the data you're able to gather through other formal and informal benchmarking activities, you end up with a data-driven strategy that always delivers the most current and relevant results.

Next Steps:

1

Make a list of 10-20 peers, competitors, or industry leaders to use for benchmarking purposes.

2

Pull the target companies' ratings from your security ratings platform. Run a report to see how their ratings compare to your own.

3

Take a closer look at the competitors who are outperforming your organization. Notice in which specific areas they're excelling.

4

Use this data to set actionable goals for improvement.

The No-Guesswork Approach to **Reporting**

As we discussed earlier, other executives and the Board of Directors need answers to key questions involving cybersecurity.

Traditionally, however, this has required the CIO or CISO to either **(1)** make a report based on their own idea of how things are going, or **(2)** report using specific, technical data.

Both of these methods have obvious pitfalls. A CIO that relies on their own judgement instead of deferring to data is more likely to be held accountable if something goes wrong. On the other hand, presenting specific technical data can do more harm than good — without the background to understand them, decision makers may over or underreact to the numbers.

USING SECURITY RATINGS FOR DATA-DRIVEN REPORTING

Security ratings are the long-awaited solution to this problem. While they rely on specific, technical metrics on the back end, the ratings themselves are as easy to understand as a credit score. Given the additional context of key competitors' ratings or an industry average, Board members, the CEO, and others can immediately get a handle on their organization's cybersecurity performance.

BITSIGHT

This provides **a new toolkit** for the CIO or CISO when negotiating for higher budgets, personnel increases, or requesting a new software tool.

On a more personal level, using security ratings in reports can help the leader of the security program prove their value to the organization by demonstrating **real**, **measurable improvements**.

Next Steps:

1

Introduce your Board or fellow executives to the idea of security ratings.

2

In your next report, include your current security rating, the security ratings of your industry or key competitors, and your plans for improvement.

3

In future reports, refer to security ratings as the central KPI of the cybersecurity program.