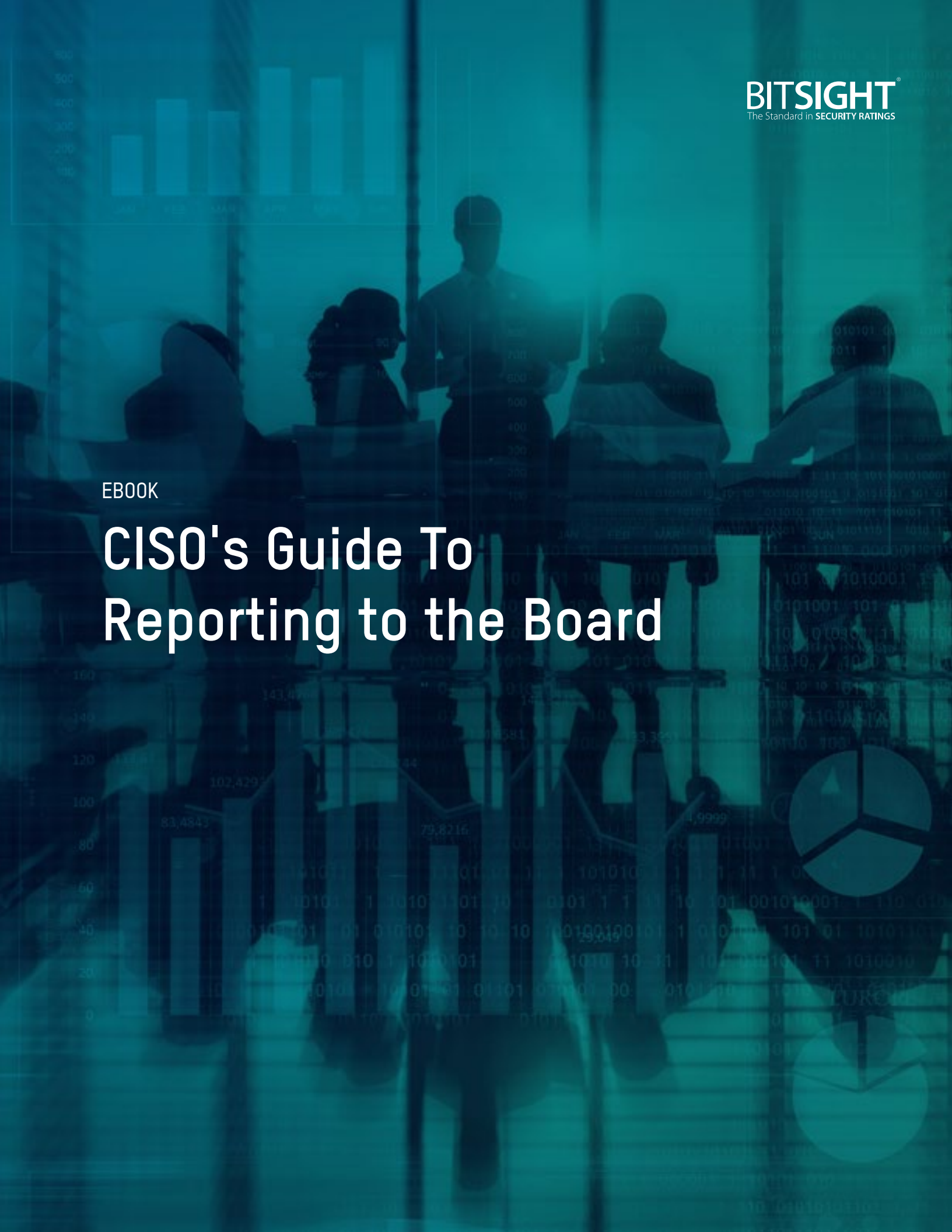

BITSIGHT
The Standard in SECURITY RATINGS

EBOOK

CISO's Guide To Reporting to the Board

INTRODUCTION

Not long ago, a board of directors would meet once or twice a year to be briefed on cybersecurity, check the box, and move on. Cybersecurity was little more than an afterthought, and mostly a box checking exercise for compliance or to make sure the bases were covered in the wake of a newsworthy event. With little technical understanding at the board level, many were happy to simply throw money at the problem and leave it to IT professionals to handle.

But the world has changed substantially in recent years, and some of the most dramatic changes have only come in 2020. Malicious actors are growing more sophisticated. The attack surface and vendor ecosystems have rapidly expanded, refocusing the security conversation towards digital risk and risk tolerance. Despite large investments in cybersecurity, the frequency and severity of attacks has not decreased—the tactics have simply evolved.

To that end, according to Gartner[1], there is also increased scrutiny from senior executives and board members on what the return of investment on years of heavy spending on cybersecurity has been. There's never been a more important time for security and risk professionals to effectively measure, manage, and communicate their security program to senior executives, board members, and external stakeholders.

In this guide, we'll arm you with information to help you before, during, and after your next board presentation.

Along with giving you best practices on objectives and presentation style, we'll give some insight into what the board is looking for and explain how to select and discuss cybersecurity metrics. Whether you're a CISO, a member of a security team, an advisor, or a board member yourself, this information is critical to your company's sustained security posture.

[1]Gartner, The Urgency to Treat Cybersecurity as a Business Decision, Paul Proctor, 22 Feb 2020

ROLES OF THE BOARD & CISO

Before preparing for your board report, it's important to understand what the roles and responsibilities are for both yourself and board members.

While many board members want to be focused on cybersecurity, they may feel completely mystified by the topic. Many don't have the background they need to talk about it with confidence or can't give it the time it needs—which is actually ok, so long as the board understands what their role in cybersecurity is.

The board is not a passive entity when it comes to cybersecurity, merely waiting to consume reports and be told how they are doing. The board's primary job is to help set the organization's security strategy, and it is the CISO's job to implement it. When we say the board is responsible for strategy, we do not mean they are responsible for choosing the right security tools or architecture. What we mean is they are responsible for identifying what needs to be defended and how important it is. Whether it's intellectual property, trade secrets, or financial transactions, the board needs to identify what the high level priorities are.

Role Of The Ciso

It is the responsibility of the CISO to work with the various stakeholders to create a plan to protect those assets, and a strategy to implement. CISOs should take a leadership role in convening stakeholders, soliciting feedback, and helping develop the overarching security protection plan.

ESTABLISH THE ROLE OF THE BOARD DURING AN INCIDENT

You need to be sure that everyone on the board knows what to do if a breach does occur. The best way to establish the role of each board member during a cybersecurity incident is to practice.

- **Create an incident response team with one board member, the CEO, and their team**
- **Review plans to notify law enforcement, forensics firms, customers and investigators**
- **Assign any additional responsibilities to board members and upper management as necessary**
- **Run table top exercises either annually or bi-annually to test preparedness**

By running a tabletop exercise before a breach occurs, you'll be able to prepare board members for what their role will be.

PREPARING FOR YOUR PRESENTATION

One of the CISO's primary roles is to convey information about cyber risk to the board of directors. But to do this effectively, the CISO needs to be able to convey security risks in business terms and help the board understand how cybersecurity impacts the company directly.

Before preparing for your board meeting, you need to think about which type of meeting it is. Each type of meeting below requires a very different presentation style and set of metrics, and it's important to know what the board typically expects to hear in each meeting.

1. **New CISO meeting the board for the first time**
    a. As the cliché says, it's hard to undo a first impression. In this first meeting the board wants to hear your assessment of the current state, what is working, what needs to change, what your goals are, and what you need to get it done. It's key to convey that you have command of the situation, and more importantly, a vision for the future.
2. **Budget justification and review**
    a. As we noted in the opening, boards are more focused on the ROI of security spending than ever. Not only do they want to see results, they want to see results related to business outcomes. Work with partners across the business, in marketing or HR for instance, to understand how improvements to security process or programs have reduced risk and enabled business growth.
3. **Annual planning and strategy meeting**
    a. The most important thing for a CISO to convey in annual planning or strategy meetings is that they are synced with the needs of the business, the strategy ladders up to the organization's larger corporate goals and objectives. For example, if one of the goals is to have 50% of digital assets move to the cloud by EOY, the CISO should present a plan to facilitate that goal by de-risking the process and improving the vendor procurement and onboarding time. The CISO, board, and upper management should leave this meeting aligned on what the CISO's annual goals and KPI's are, including security rating improvements, comparison to competitors, and time to address vulnerabilities or system intrusions.
4. **Monthly or quarterly status**
    a. In your status updates, you shouldn't only focus on your attainment to goal. The board wants to hear what you're prioritizing and why. Have there been unforeseen dependencies? Has the situation on the ground changed and required a shift in priorities? Do you have the personnel and budget to execute on everything that needs to be done? Also consider sharing updates with the board about recent sector or national incidents and how the company would be prepared to respond to them.
5. **Event-driven board meeting**
    a. This may be the most stressful type of meeting, but if you've done your tabletop exercises, you should be ready. In this meeting the roles and responsibilities of each member of the board and upper management should be clear. Be prepared to succinctly speak in non-technical language to what happened, what it means, and how it can be solved.

All in all, the primary question remains: "Are we taking the right actions to reduce risk?" Today's board member understands that poor security performance has far reaching impacts from reputational damage, to lost business to impacts on stock price.

The CISO needs to be able to communicate how the program is reducing risk, and how it is an active enabler of the business.

DURING YOUR CYBERSECURITY PRESENTATION TO THE BOARD

You need to know how to present this information. What tone will you take? What are your primary goals and objectives?

There's two parts to each board meeting: the Style and the Substance.

Style

When thinking about the style of your presentation, it helps to consider how you're comfortable presenting information, and how the board likes to consume it. The goal is to create an experience that feels natural and easy to follow. Building slides with simple graphic-based charts or dashboards and only 3 or 4 bullets is usually the best way to facilitate conversation. If you have in depth spreadsheets, call out some highlights, but distribute as an appendix for the board to review on their own. Be sure to ask the company's CEO, corporate secretary, or other knowledgeable executive about how the board prefers to consume materials.

Substance

When it comes to substance, think of your job in this meeting as telling a story. You need to educate the board on the organizations' cybersecurity posture, why you chose the metrics you did and what they mean for the business, how the personnel and the budget could affect those metrics.

And most importantly, what will you actually present that will prepare the board with the information they need to know?

Here are a few suggested topics to cover in each type of meeting.

New CISO meeting the board for the first time

1. What is your assessment of where we are now?
2. How do we benchmark against others in our industry or peer group?
3. What are the KPI's we should be looking at?
4. How do those security KPI's correlate to business outcomes?
5. What should we be doing differently to meet those KPI's?

Budget justification and review

1. How much have we spent this year vs last year?
2. Review of KPI's
3. Roll up of ROI (how did security improve/not improve relative to spending)
4. Business impact (how did security enable the business to grow?)

Annual planning and strategy meeting

1. Review of organization's overall strategy and plan and how security fits into it
2. Review of focus areas from last year
3. KPI update
4. Current benchmarking against competitors and peers
5. Changes to risk profile
6. Findings of independent assessments
7. Focus areas for the new year
8. Which areas of the business will be most impacted
9. Budget requirements
10. Projected KPI's and results

Monthly or quarterly status

1. Review of KPI's and highlights from last meeting
2. Benchmarking update
3. Major wins/losses to date
4. Upcoming initiatives
5. Changes to risk profile

Event-driven board meeting

1. What happened?
2. What is the impact?
3. Is there a regulatory issue?
4. Have others in the industry been affected?
5. What remediation efforts have been undertaken?
6. Projected time to resolution
7. Expected outcome

Now you know what the board is looking for here's a few things to keep in mind:

Resonance: Making sure the material you're presenting resonates with the board is imperative. Make sure you're using non-technical language and focusing on strategy and risk, not "bits and bytes." As Forrester noted in a recent study[2], "For example, we found that 63% of firms that measure the number of blocked malware incidents also report the metric up to the board. But because this metric provides no larger context and is subject to analytical bias, it is inappropriate for strategic board-level discussions."

Transparency: The board needs to know flat out how the company could be affected by its cybersecurity posture. Cybersecurity is a company-wide issue, so the board should see how it could potentially impact every aspect of business.

Boundaries: It is not up to you as the CISO or CIO to determine what risks the company is willing to run, but it is your responsibility to be fully aware of the risk tolerance the board is comfortable with.

TIPS FOR PRESENTING THREATS TO THE BOARD

As a CISO, you're concerned with gathering threat intelligence information using a variety of methods. When you've gathered information about a credible threat or threat actor, you'll need to be prepared to share that information with the board.

Presenting threats is a great way to show that you're paying attention to the health of the company and lends to your credibility. But you need to be able to show the board that this information is real and could very potentially make a marked impact on the organization.

[2]*Forrester, Better Security And Business Outcomes With Security Performance Management, September 2019*

Tip #1: Don't spend time trying to explain who (or what) may pose a threat. Cybersecurity is dynamic and is always changing and evolving—so frankly, that isn't relevant.

Tip #2: Address the issue, and get right to discussion about mitigation. Don't just present a problem—bring a solution.

Tip #3: Provide the board with actionable insights backed by data. (We'll discuss what those metrics might look like next.)

Metrics: How To Select & Present Them

Knowing the best practices on how to present cybersecurity to the board is one thing—but without substantive data, you won't have a very compelling (or helpful) presentation.

The first thing you need to keep in mind regarding metrics is context. Board members likely don't know what it means if you say that "500,000 intrusions hit the detection system." You need to focus on being concise with your explanation and show them how the metric impacts the health of the company. You'll want to focus on showing metrics over time that

demonstrate if you're getting better and anything that shows cause and effect.

Determining Which (& How Many) Metrics To Present

Remember, the board doesn't have the time to learn about every metric you track. The metrics you select should provide context, gain traction, and tell a story.

As Dmitiri Alperovitch, co-founder of Crowdstrike put it, "the responsibility of the board is not be involved operationally and tell the CISO which firewall to buy and which technology to deploy, but it is their responsibility to hold them accountable and make sure they have the resources needed."

According to recent Forrester Consulting report — Better Security And Business Outcomes With Security Performance Management[3] — the most common metrics reported to the board are as follows:

- 50% Number of malware incidents blocked
- 50% Percentage of intrusions blocked by firewall/network security
- 45% cybersecurity ratings
- 45% Percentage of phishing/malicious emails filtered
- 40% Number of data loss prevention (DLP) incidents generated

[3]*Forrester, Better Security And Business Outcomes With Security Performance Management, September 2019*

But Forrester is also clear — 4 of these metrics don't meaningfully communicate exposure or performance — they are specifically measurements of our own efforts and don't put it into broader context. And Forrester says that CISOs should think twice about reporting them to the board.

Forrester highlights security ratings as a more appropriate metric for board-level communication because ratings are risk-focused, objective, and outcome-based.

Tip: We suggest beginning with a small number of metrics at the beginning of a quarter or year—maybe four or five in each category below. Begin introducing them to the board, and track their success during the year. Four quarters later, when the board is comfortable seeing those metrics and their result over time, you can add another few.

There are two broad categorizations of cybersecurity metrics that you might present to the board: audit and compliance metrics and operational effectiveness metrics.

Category #1: Audit & Compliance Metrics

Some companies have a legal requirement to be audited with respect to IT security, making audit and compliance metrics highly relevant and important.

Some examples include:

- "Are we ISO-27001-compliant?"
- "Do we have a vendor risk management program?"
- "Do we have any outstanding high- risk findings open from our last audit or assessment?"
- "What percentage of the NIST framework are we implementing?"

The NIST framework has roughly 80 questions associated with it. If a board member asks if you're doing the NIST framework, you might say, "Today we're doing 60% of it."

Tip: You're likely going to be asked by the board about some audit and compliance metrics, so there are good reasons to be prepared to talk about them. But as a CISO, you also need to be able to pivot and say, "These are important questions, but they don't tell you what is actually happening in regard to cybersecurity." And that is where operational effectiveness measures come in.

Category #2: Operational Effectiveness Metrics

These are quantitative, no-kidding, reality- of-the-situation-type metrics. Operational metrics are backed with actionable data. Examples include:

- "How may intrusions were detected this year?"
- "How quickly are we detecting, investigating and remediating threats?"
- "How much have we spent this year?"
- "How many vulnerabilities were in our network and how quickly were they fixed?"
- "How many compromised systems did we have compared to last year?"
- "Has our risk profile changed?"
- "How did we compare to our peers across X time span?"

BitSight Security Ratings allow you to easily compare your performance to a number of your competitors over a period of time.

> **Being able to show our board, leaders, and even customers and partners how Veracode is performing over time and relative to others in our space is a powerful tool for communicating our commitment to security excellence, and has also become a terrific competitive differentiator."**
>
> - Bill Brown, CIO and CISO, Veracode

How & When To Ge Additional Details

Keeping your metric explanation brief is ideal—but some members of the board may want to go deeper. This is where an appendix comes in handy. With an appendix, you can easily tell the board members to flip to a particular page for more detailed information, which they can review during or after the meeting.

Tip: Any metric that doesn't merit a "yes/no" or "red, yellow, green" status- indicator answer should be accompanied by a visual. For example, the peer benchmarking example we showed

on the left demonstrates a dynamic, performance-based comparison over time and is very helpful for the board.

CONCLUSION

Cybersecurity has only recently come into the spotlight for boards. Today, it is considered a critical aspect of company operations by the board of directors.

The modern CISO must be able to make the case for how cybersecurity impacts their business directly—and one of the most effective ways to accomplish that is through data. This is where BitSight can help.

If you want to see how BitSight's Security Rating platform can monitor your (and your vendor's) cybersecurity performance—and give you the tools you need to create compelling metrics at the click of a button—request a FREE demo today.

REQUEST A DEMO

BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Seven of the top 10 largest cyber insurers, 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit **www.BitSight.com**, read our blog or follow **@BitSight** on Twitter.