# REPORTING CYBERSECURITY TO THE BOARD

## A CISO'S GO-TO GUIDE

BITSIGHT®
The Standard in SECURITY RATINGS

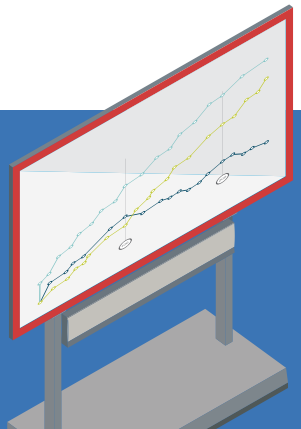
# INTRODUCTION

**Ten to 15 years ago, a board of directors would meet once or twice a year to be briefed on cybersecurity, check the box, and move on. Back then, cybersecurity was little more than an afterthought.**

After Target's 2013 data breach, advisory firm Institutional Shareholder Services recommended that seven of the 10 board members be replaced for failing to adequately oversee cyber risk as part of their duties.[1] This report signaled a major shift in corporate cybersecurity policy. Since then, there's been a heightened interest in securing a company's data, and more senior-level responsibilities for cybersecurity are in place.

**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 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]http://www.bloomberg.com/news/articles/2014-05-28/target-investors-should-replace-seven-directors-iss-says



# COMMUNICATING WITH THE BOARD: A PREFACE

**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.**

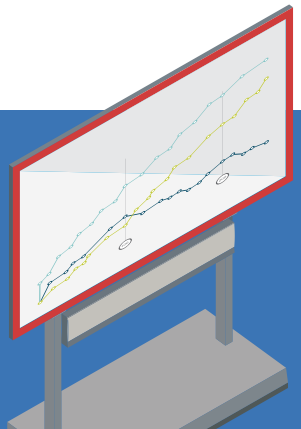
The board has to think about many angles in regard to cybersecurity:

- Regulation: Are we meeting our regulatory requirements?
- Fiduciary duty: Are we acting appropriately with regard to cybersecurity for our customers and shareholders?
- Company liability: If we perform poorly in cybersecurity, how does it affect our business performance overall?
- Personal liability: If we perform poorly in cybersecurity, how does it affect my position as a CISO?

All in all, the primary question remains: "**Are we taking the right actions to be secure?**" Today's board member understands that a data breach could lead to fines, lawsuits, reputational damage, and even termination.

But 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.

**The CISO needs to be able to communicate that you cannot prevent all bad things from happening to your network or your data—but the damage can be mitigated through taking the right steps.** The board should be more focused on eliminating catastrophic damage and less focused on worrying that something might happen to the network.



# BEFORE & AFTER YOU PRESENT CYBERSECURITY TO THE BOARD

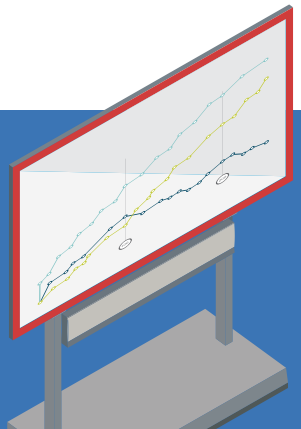
**Cybersecurity doesn't start (or stop) when you enter (or exit) the boardroom. There are several important tasks that should take place before and after boardroom presentations.**

## DETERMINE WHO SHOULD PRESENT TO THE BOARD AND AT WHAT FREQUENCY.

Of course, a great deal of this determination will be based on the structure of your organization. And while these may be things you've already determined, they might be worth revisiting.

- **Presenting solo:** If you're given a very limited amount of time for your presentation, it may be best to cover everything on your own. Furthermore, some boards like reports to come from the head of a department only. Either way, make sure you're comfortable handling the presentation on your own if necessary.
- **Co-presentations:** Sometimes you may present with the head of compliance or the director of marketing, for example. This type of integration can be effective to demonstrate to the board that security has been broadly integrated.
- **Third-party presentations:** At times, consultants are brought in by the board of directors, the general counsel, or the CEO to provide an external perspective. This individual may actually be helpful to you as the CISO, as they may be able to use their experience in your industry to help with benchmarking. When third parties are brought in, the board typically wants to know if the company is performing well or not relative to other organizations.

The frequency at which you present to the board is always determined on a case-by-base basis. You could present quarterly, bi-annually, or annually, depending on your company culture, industry, and a number of other factors.



## ESTABLISH THE ROLE OF THE BOARD DURING AN INCIDENT.

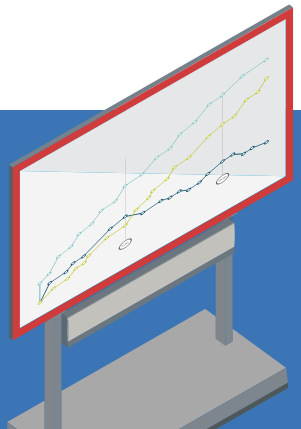
Your first goal should always be to prevent and detect security breaches—but you won't be able to stop them all. This is just a part of the threat landscape today. It's important to adopt a mentality of "not if, but when." So you need to be sure that everyone on the board knows what to do if a breach does occur.

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

This is not an implementation that should be set in place during the first breach your organization encounters. If you wait for that, you're going to experience mass confusion and frustration.

The best way to establish the role of each board member during a cybersecurity incident is to practice. By running a tabletop exercise before a breach occurs, you'll be able to prepare board members for what their role will be. It's important that everyone in upper management knows how to respond and that plans are in place for notifying law enforcement, forensics firms, customers, and investors to help deal with potential financial and reputational harm.

Not all board members need to be directly involved during a breach—just one member of the board, the CEO, and their team will suffice. The rest of the board members should have assigned responsibilities and objectives to be working on. After walking through these tabletop exercises, you (and your upper management) will feel ready to take care of a problem right away.



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

You'll need to determine both your **goals and presentation style** as well as the **content of your presentation**. Let's start with the former.

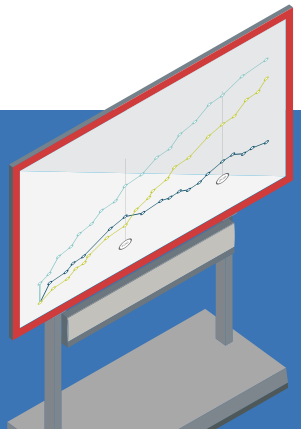
## GOALS & PRESENTATION STYLE

### What The Board Wants To Hear

There are two categorizations the board will be interested in learning about: **compliance** and **actual security**. You and the board both know that there is a big difference between the two. You may be complying with a particular set of security standards, but that certainly doesn't mean your network won't be compromised.

To that point, the board will want to know if you're just checking boxes or if there is an actual strategy in place. If there is a strategy in place, they'll want to know the exact steps you're taking to achieve your goals.

There are two categorizations the board will be interested in learning about: **compliance** and **actual security**.



## What The CISO Should Focus On

Now you know what the board is looking for—so what should you focus on during the presentation?

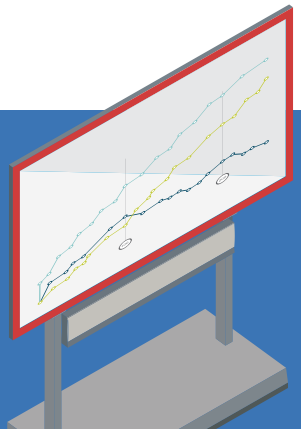
- **Resonance:** Making sure the material you're presenting resonates with the board is imperative.
  - **Tip:** Consider looking at recent breaches in your industry and running through how your company would have fared in each particular situation. This will make the threats "real" and will put them in perspective.
- **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.

> ...it is your responsibility to be fully aware of the **risk tolerance** the board is comfortable with.

## Building Credibility With The Board

**Tip #1:** Make sure the board understands you're there to support the business and that the cybersecurity protections necessary are in place to protect the organization's ability to function appropriately.

**Tip #2:** Let the board know that you're there to help facilitate decision-making to determine what the risks are and how to mitigate them.



**Tip #3:** Find one member of the board who is willing to be your champion. This individual should be interested in learning about cybersecurity and willing to spend time on this topic outside board meetings. You can't educate the entire board on every topic, so this person will help you establish credibility with the other board members.

**Tip #4:** Create a cybersecurity or IT committee. Even better than having one champion is having a whole group! If there are enough board members interested, feel free to have an open dialogue about security at all times.

**Tip #5:** Talk to the board in their language—cut out any cybersecurity jargon. Talk in terms of risk management, stock price, and bottom line.

## Presenting Threats To The Board

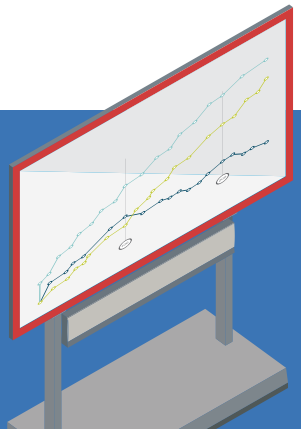
As a CISO, you're concerned with gathering threat intelligence information using a variety of methods. When you've gathered information about a credible threat or threat actor, you'll need to be prepared to share that information with the board.

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.

**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.

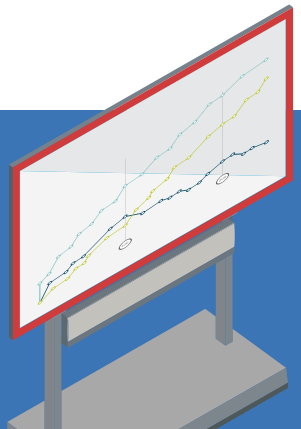
**Tip:** We suggest beginning with a small number of metrics at the beginning of a quarter or year—maybe four or five in each category below. Begin introducing them to the board, and track their success during the year. Four quarters later, when the board is comfortable seeing those metrics and their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



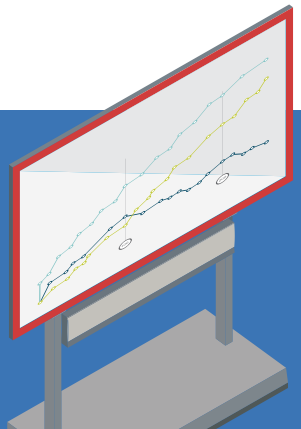
- **"Do we have any outstanding high-risk findings open from our last audit or assessment?"**
  - This is subjective. What really constitutes "high risk"? Even if you complete the high-risk findings, something bad could still happen on your network or to your data the next day.
- **"What percentage of 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.

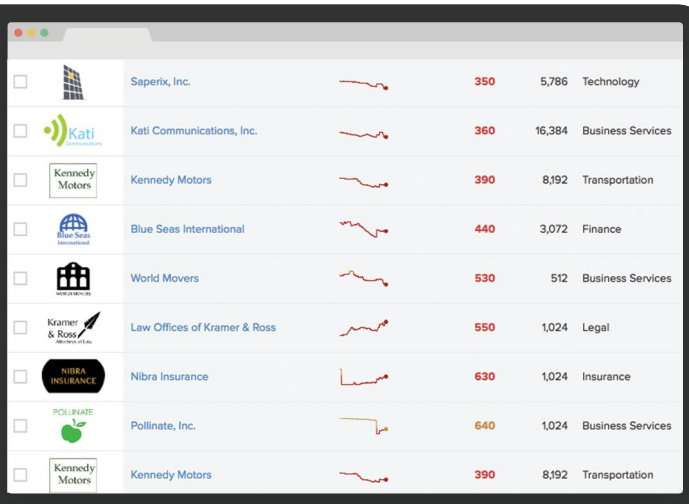
## Category #2: Operational Effectiveness Metrics

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

- **"How quickly can we remove employee network access?"**
- **"How quickly can we (or our vendors) identify and respond to incidents?"**
- **"What percentage of our users click on spear-phishing training emails?"**
  - It's very common for IT security teams to send out fake phishing emails to employees. If the employees click on them, a screen may pop up and explain that what they've done is a major security issue. From an operational standpoint, this metric gives your team some real insight into internal security practices.



- **"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. The image below shows the graphic comparison you could generate for your board with the click of a button.

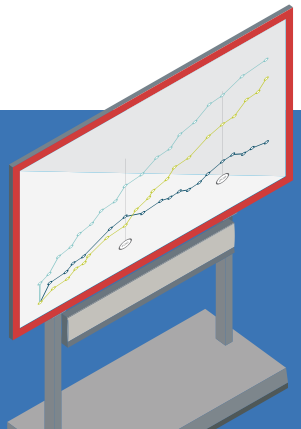



The portfolio level view in the BitSight Security Ratings portal.

## How & When To Give 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.



# IN REVIEW

**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 FREE DEMO