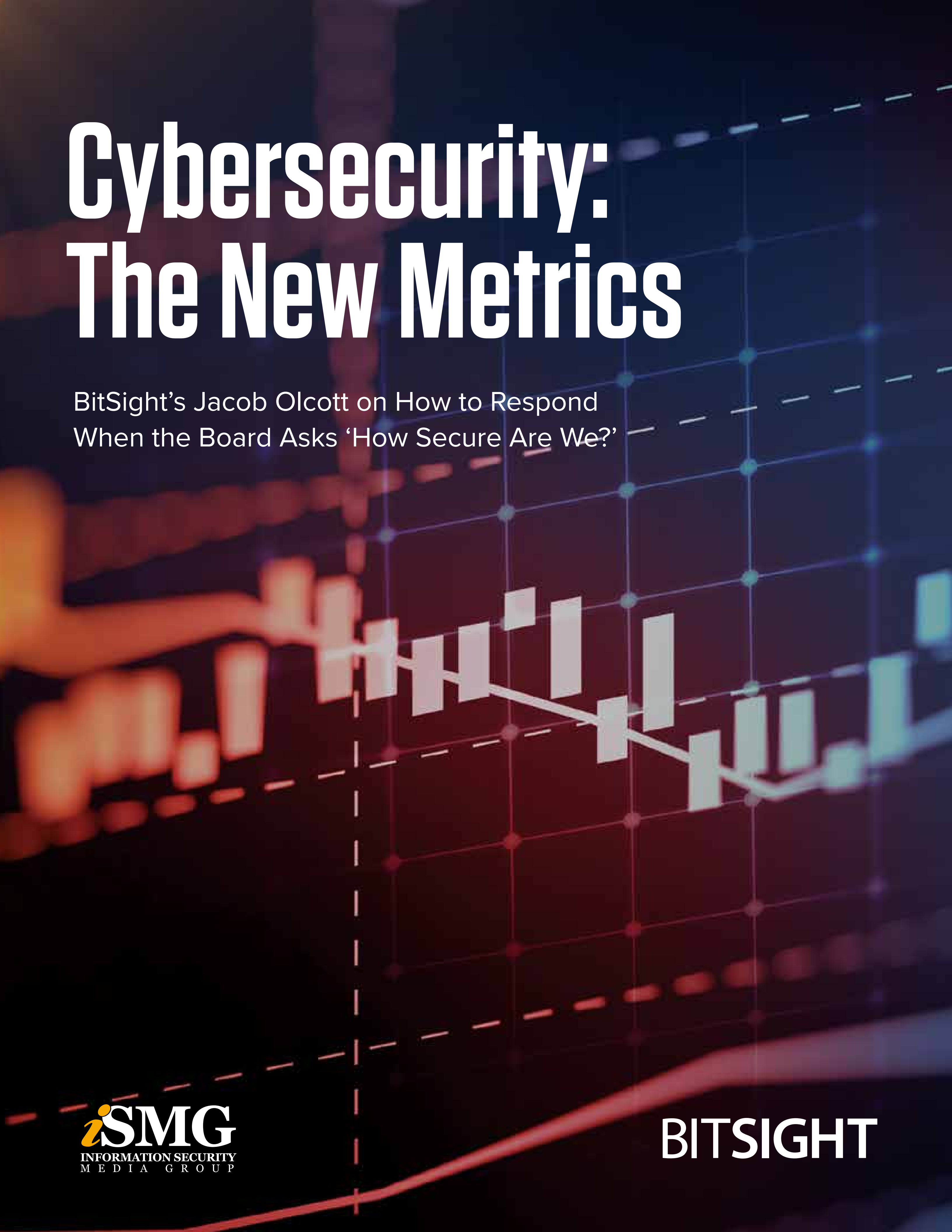
Cybersecurity: The New Metrics

BitSight's Jacob Olcott on How to Respond When the Board Asks 'How Secure Are We?'



iSMG
INFORMATION SECURITY
MEDIA GROUP

BITSIGHT

“How secure are we?” That’s one of the most common questions asked by boards and senior managers. But security and technology leaders do not always have ready answers, says Jacob Olcott of BitSight Technologies. Are they even using the right security metrics?

It’s a real and growing challenge, says Olcott, BitSight’s Vice President of Business Development.

“The challenge that CIOs and CISOs face is to be able to take what is a very complicated process with lots of different metrics and measurements and distill that information in a way that can be consumed by senior executives and the board, so that they can understand if they’re meeting the standard of care in our industry. Are we performing adequately, or do we need to be investing more resources to improve our own defenses?”

And a common problem, Olcott adds, is that security and technology leaders often rely on the wrong metrics.

“I think people get caught up in only collecting what I refer to as the audit and compliance metrics,” he says. “And they miss the opportunity to collect what is actually maybe even more significant, which is the operational effectiveness measurement.”

In an interview about cybersecurity metrics, Olcott discusses:

- What’s wrong with traditional metrics;
- How good metrics help benchmark against peers and rivals;
- Do’s and don’ts for presenting security metrics to the board.

Before joining BitSight, Olcott managed the cybersecurity consulting practice at Good Harbor Security Risk Management. Previously, he served as legal adviser to the Senate Commerce Committee and as counsel to the House of Representatives Homeland Security Committee. He completed his education at the University of Texas at Austin and the University of Virginia School of Law.

Jacob Olcott

‘Are we secure enough?’

TOM FIELD: Jacob, security and technology leaders frequently are asked the questions, “How secure are we?” and, “Are we secure enough?” In your experience, how are they currently answering those questions?

JACOB OLCOTT: Bottom line: They’re having a really hard time answering the question. As everybody knows, cybersecurity has become one of the most important issues of discussion among senior executives and board members.

There’s a pretty clear reason why that is. Look at the Yahoo breach and its impact on the Verizon acquisition. We can see this is a very important issue to the bottom line. A lot of money is at stake, and organizations that do not adequately or effectively secure themselves can get hurt in the process.

Senior executives are asking their CIOs and their CISOs to report to them on the effectiveness of their cybersecurity programs. The challenge that CIOs and CISOs face is to be able to take what is a very complicated process with lots of different metrics and measurements and distill that information in a way that can be consumed by senior executives and the board, so that they can understand if they’re meeting the standard of care in our industry. Are we performing adequately, or do we need to be investing more resources to improve our own defenses?

> “Senior executives and board members are very concerned about whether they are meeting the industry standard of care.”

The Problem With Traditional Metrics

FIELD: Jake, clearly this is something leaders have thought about in the past. Tell me, what’s wrong with the traditional metrics they have tried to use?

OLCOTT: I think people get caught up in only collecting what I refer to as the audit and compliance metrics. They miss the opportunity to collect what is actually maybe even more significant, which is the operational effectiveness measurements. When we talk about audit and compliance metrics, we’re really talking about whether we are compliant with an international standard, or we resolved any outstanding issues from a previous audit, or we are compliant with what percentage of pieces with respect to an industry framework, or something like that. All of these things are very important metrics for a CISO or CIO to be collecting.

Really, you want to collect more operational effectiveness metrics. These metrics are specifically about risks to our environment, results from penetration tests or vulnerability scans, or the ever-important metrics about time to detection and time to remediation, the time that it takes to remove access of employees off of our network, and things of that nature. Traditionally the approach has been: “Let’s just collect the audit metrics and report those up to the board.” We’re finding a shift now where more senior executives and CEOs want to dive deeper into performance measurements and metrics. The questions that they’re asking are more about operational effectiveness rather than a check-the-box audit and compliance regime.

Getting the Board’s Attention

FIELD: Jake, what operational metrics will really get management’s and the board’s attention?

OLCOTT: I think the metric that most cybersecurity programs hold themselves to is the detection deficit gap. It’s a very well-known metric that has been reported for years by the Verizon data breach report and the Mandiant report, among others. It essentially measures the time it takes an organization to identify some piece of malware that exists inside of its network and then to tick it off of its system. The reason it’s so important is because the longer a bad guy can dwell within your organization, the more likely he or she is able to steal a lot of your sensitive data. It’s very important to reduce that time to identify and time to remediate as far down to zero as you possibly can. That’s a very important metric for senior executives and board leaders.

> “BitSight enables organizations to observe ratings of other peers, competitors and industry standards, and do so in real time.”

The other really important measurement we’ve observed at BitSight over the last few years is how an organization compares its cybersecurity effectiveness to its peers and competitors in its industry. Senior executives and board members are very concerned about whether they are meeting the industry standard of care. It means they are performing along with their peers and competitors; those peers and competitors are not overperforming on cybersecurity compared to them; and that they have invested the time and tools and technology into building an effective cybersecurity program. BitSight provides these ratings that will allow organizations to compare themselves to others.

The Importance of Benchmarking

FIELD: Jake, it’s great to use these to answer the questions that we talked about, but metrics can also help organizations benchmark against their peers and competitors. Tell me how they do that and the value of that, please.

OLCOTT: Historically, it’s been very difficult to benchmark yourself against other organizations because the way an organization would approach cybersecurity benchmarking would be to collect qualitative, subjective data through questionnaires, peer review groups or things of that nature. You would get an idea about the types of programs that other folks might have in place in other businesses in your same sector, but you would never really know exactly how effective those programs were.

BitSight enables organizations to observe ratings of other peers, competitors and industry standards, and do so in real time. BitSight produces security ratings that are of the quantitative, objective variety. We’re measuring infection rates and time to identify and remediate issues. Organizations are able to get much more in-depth quantitative data about their security posture as it compares to others in the industry, which is very useful especially in conjunction with what we would think of as qualitative, subjective data that they collect by engaging in information sharing groups and other questionnaire-based approaches to benchmarking.

"Don't overwhelm people. Management, senior executives and board members are already overwhelmed with lots of different key data points about a variety of issues."

FIELD: Jake, I could see where it would be tempting for a technology or a security leader to overwhelm management or the board with metrics. What would you say are some of the dos and don'ts when it comes to presenting these metrics to the board?

OLCOTT: No. 1: Don't overwhelm people. Management, senior executives and board members are already overwhelmed with lots of different key data points about a variety of issues. Cybersecurity is something that's still fairly new for a lot of executives and board members. So, it's very important to collect high-quality metrics and present a limited number of those high-quality metrics to the board at any given time.

No. 2: Do present only the most relevant or material data to the board. The ways in which you present the effectiveness of your cybersecurity program, as well as the designs being used, is also important.

No. 3: Do use graphics and other comparison data that you can provide to those board members as opposed to just the ones and zeros. Breaking things up in a Word document is not the best approach. You want to be a bit more visual in the way that you represent some of this information.

How BitSight Can Help

FIELD: Jacob, talk to me about BitSight. How are you helping organizations to gain a clearer picture of their own security postures?

OLCOTT: BitSight provides security ratings on organizations. Those security ratings are provided in real time. Organizations use our ratings for a variety of purposes including third-party risk management, underwriting cyber insurance, doing due diligence in an M&A contest and, of course, benchmark comparisons, as we've just discussed. I would encourage anybody who's interested in any of those ideas to come check us out and allow us to show you what we got.

http://www.bankinfosecurity.com/interviews

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
sales@ismgcorp.com

BANKiNFO SECURITY® CUiNFO SECURITY® Just for Credit Unions GOViNFO SECURITY® HEALTHCAREiNFO SECURITY®

iinfoRisk® TODAY CAREERSiNFO SECURITY® Data Breach. Prevention. Response. Notification. TODAY

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com