WHEN SECURITY METRICS MISS THE POINT

BY GUEST AUTHOR: JOHN MASSERINI, CISO, MILLICOM (TIGO) COMMUNICATIONS

Three-time CISO John Masserini, shares his opinion on the complex topic of information security metrics.

In today's world, many of us have heard of the Body Mass Index (BMI) and likely have had some intense discussions with our healthcare providers about our personal BMIs. The idea behind BMI is that a 'healthy' person of a given height should be within a range of upper and lower weights. A well-intentioned effort to give the general population an understanding about what their 'optimal' weight should be. But looking closely, BMI is nothing more than a metric used by the medical profession to put some type of measurement on a person's weight/height ratio. Unfortunately, the BMI calculation doesn't consider the type of weight a person carries – whether its fat, muscle, or water – only that they have it. Because of the lack of context behind the BMI, it can be misleading around a person's true health status. For example, every world class bodybuilder, all who average 3%-5% body fat, are all morbidly obese according to the BMI. Kind of strange in my opinion.

Now, I'm sharing all of this to prove an important point that every security executive needs to come to terms with: even though they are well intentioned, just like the BMI, security metrics can be horribly misleading.

Don't get me wrong. I am a huge advocate of measuring your security program and leveraging those metrics to communicate risk with all of your stakeholders. That said, all too often those metrics are used for shock and awe rather than communicating important messages around risk.

After countless years of presenting to boards, executives, and colleagues, I've found that I've developed almost a split-personality when I'm asked about what metrics to track. There are metrics that I need to manage risk across my enterprise, and there are different metrics that my executives are interested in. Sometimes they are the same, but most times they are not.

OPERATIONAL VS. RISK METRICS

When running an operation whose sole focus is on defending us against attacks, the kinds of metrics I want collected are of very little interest to my board. I care about ensuring I have enough headroom with my solution as much as the amount of risk I mitigate. We shouldn't be bragging when our solutions are doing what they are supposed to – only highlighting when they don't.

If you feel compelled to talk about the shock and awe numbers, do yourself (and your board) a favor and talk about efficacy – not volume. Telling your board that your anti-SPAM solution is 99.9735% effective means far more to them than saying you blocked a gazillion SPAM emails, and as a side benefit, you get to open up a dialog with them around how no solution is 100% perfect.

Your goal is not to use metrics to scare your executives, but to find metrics that they can relate to. To quote one of the most influential psychiatrists of the 20th century, Milton Erickson once said:

> *"Every person's map of the world is as unique as their thumb print. There are no two people alike. No two people who understand the same sentence the same way... So in dealing with people, you try not to fit them to your concept of what they should be."*
>
> \- Milton Erickson

Ponder that for a moment. Most of us deal with boards and management teams which number in dozens of participants. Your metrics need to make sense not to the one person you are speaking to, but the dozen or so board members who all come from diverse backgrounds and experiences. You don't have one different map of the world to deal with, but dozens. Well planned metrics bridge the communications gap that comes with having multiple world maps in your boardrooms.

OPERATIONAL METRICS:

So even after all of this, I admit I do share certain operational metrics with my executives and board.

SOC EFFICACY: Metrics like Mean Time to Close (MTTC)/Mean Time to Resolve (MTTR) reflects the efficiency of the SOC team in resolving events. This is a key indicator of staffing challenges in the SOC and highlights the potential need for hiring or training existing staff. The key is to choose metrics that not only measure risk reduction, but also demonstrate value and effectiveness.

COMPOUND ANNUAL GROWTH RATE OF EVENTS AND INCIDENTS: In the financial world, CAGR is a common term with a well-defined meaning. By using this metric to represent the growth of events, incidents, and attacks, executives understand the reasoning for budgetary investments in the security infrastructure and SOC. Used hand and hand with the MTTC metric.

SOLUTION EFFICACY: The overall effectiveness of the existing solutions. This is where we measure SPAM, NIDS/NIPS, Anti-Virus and any other solution we have deployed. This is also used to show the adoption rate of new measures like multi-factor authentication, privileged access management, and user certification hygiene.

SOLUTION LIFE EXPECTANCY: This metric shows any security solution that has less than 20% headroom is beginning to show a decreased efficiency due to changes in infrastructure, attack vectors, or business functions. Primarily used to set the stage for budgets or capital expenses.

RISK METRICS:

Ultimately, this is the bread and butter of any metrics program. Each of the categories below can leverage the same data collection for both functional risk mitigation strategies, as well as communicating those risks to executives.

ATTACK METRICS: Attack metrics are arguably the easiest to obtain and the hardest to use effectively and the most susceptible to succumb to the pitfall of shock and awe. Here's the thing about attack metrics – while the month-over-month volumetrics are important, most of the rest of it is useless noise. Discuss the new attack(s) we're seeing that we are susceptible to and what we're doing about them.

VULNERABILITY METRICS: The stalwart of the metrics world has to undoubtedly be reporting vulnerabilities. The key to effective vulnerability metric reporting is to relate them to potential financial impact to the company. Do not report a count of generic 5-tier risks (none through Critical) to the board without any insight to the financial impact of your critical systems. Again – avoid the shock and awe, but rather, put these findings into context by associating them with the revenue that could be impacted by attacks impacting those systems.

AVAILABILITY METRICS: All too often, the availability of a system is prioritized well behind the confidentiality or integrity of a system. Have you done a business impact analysis on that 30-year-old system that runs that old Cobol-68 program which just happens to drive 75% of your revenue? Well guess what? The board wants to know you're on it and there's a plan to ensure its upgraded, migrated, or backed up even though there isn't a published exploit anywhere in the world. If you've forgotten what the C.I.A. is, perhaps it's time for a refresher.

REGULATORY METRICS: We all have them – whether its PCI, HIPAA, SOX, or any other government/industry regulatory requirement we have to deal with. When discussing these risks with your board, do not just talk about the gaps you have. Make sure you also articulate the potential fines, especially in this GDPR world, and how those gaps could directly impact the levels of fines faced. It's easy to again fall into the shock-and-awe situation with this, but try to avoid it. Use as much realistic data as possible, especially when dealing with publicly disclosed fines.

So, is your next board meeting going to be filled with fear-inducing, shock and awe, BMI-type metrics, or are you going to focus on communicating those risks that the board wants to hear in a way they want to hear it?

Remember, every person in that room interprets your words in their context – not yours. Make sure your metrics bridge the maps of all the world's before you.

John Masserini is recognized as an industry leader whose expertise across multiple verticals provides a unique approach to delivering an information risk program which drives business focused solutions to today's global information security and compliance challenges. Read more of John's opinions on his blog, Chronicles of a CISO: https://johnmasserini.com