WHAT DO METRICS MEAN TO YOU?

From our in-depth analysis on metrics through countless CISO discussions, CISOs are at a turning point and for those who are not utilizing business *and* technical focused metrics, they recognize the need to start is now. In the *State of Cybersecurity Metrics Annual Report, 2018* 58% of CISOs scored a failing grade when evaluating their efforts to measure their cybersecurity performance against best practices. In that same study, 4 out of 5 companies worldwide are not fully satisfied with their cybersecurity metrics and 43% of respondents indicated some visibility into cyber security metrics but still fail to integrate business stakeholder needs when making critical decisions. When respondents were asked why their metrics fall short, the top two responses were inadequate resources (42%) and time constraints (37%). In another study: *Information Security Risk Metrics, 2017*, 25% of CISOs do not collect and report on metrics, for the 75% that are utilizing metrics, only 40% of their metrics are business-focused.

Here we share quotes we have previously published from CISOs featured in *Feats of Strength*. We asked each of them how they report on metrics and hope their responses may guide some of our readers in the right direction.

"We should really focus on key risk indicators. So how do you prove that you've reduced risk? How many assets do I have under management? How many things are at baseline? And if you can't do that, then don't buy it. So that's how I justify things with management. And I think that actually starts to make sense. As soon as you start talking about risk reduction by dollars, it becomes a lot easier. The biggest complexity was to try to make an argument for visibility because it's not as interesting. It doesn't bring down risk inherently."

– Brandon Swafford, CISO, Webster Bank (original quote from Feats of Strength, March 2019)

"I have 13 metrics that I look at on a monthly basis that either talk about the effectiveness of the program or operations. I'm trying to keep them at a high level and when we talk about metrics, a lot of people like to see colors. So, we talk about being red, yellow and green, but in a different context. Red would mean management needs to take an immediate action, yellow would mean management needs to monitor this area and green means management does not need to take action at all."

- Rich Licato, CISO, ARC (original quote from Feats of Strength, June 2018)

"We report metrics to the board quarterly. We also talk to the board about what our target state is, and where we want to be in the next two years. They absolutely want to know how we stack up against others in the industry and whether or not we're doing the right things."

- Christopher Porter, CISO, Fannie Mae (original quote from Feats of Strength, June 2018)

"I think about two factors. One is collecting true metrics around my program maturity and framework and the ability to define where I am. I need to understand that if I want to move up in maturity what that means from a policy, procedures, and budgetary perspective. The other is technical benchmarking against competitors that I can then use on my own program."

- Richard Rushing, CISO, Motorola (original quote from Feats of Strength, June 2018)

"I think it comes down to ensuring objectives are aligned on what the security organization is supposed to bring to the table. At LinkedIn, the focus is on ensuring member trust with the products we build, securing and hardening our infrastructure, and being resilient when bad things happen. It's really important as a CISO to have a very clear and crisp narrative about what those security objectives are and receive buy in from additional internal stakeholders."

- Cory Scott, Former CISO, LinkedIn (original quote from Feats of Strength, June 2018)

"[CISOs judge progress] primarily by metrics, especially when reporting to senior leadership like the Board. This is where frameworks such as the NIST Cyber Security Framework, help. These frameworks give you a model to communicate to senior leadership what you're doing, why you're doing it, and how you benchmark or measure up."

– Lance Spitzner, Director, SANS Institute (original quote from Feats of Strength, March 2019)

"KRIs are really a great way to do it. Board reporting is a challenge because every board is not created equal. Some companies I've worked for have wanted to tell the board everything. Other companies have been more about making sure that we're giving information that is relevant. Figuring out that balance with your board of how much or how little information is key."

- Patricia Titus, CISO, Markel Corporation (original quote from Feats of Strength, June 2018)

"Like everybody else, we still struggle with trying to find what the best metrics are to convey to the business. At the end of the day, it's about knowing your audience, what's important to them, and what level of detail they like. For example, I do a quarterly governance report where I focus on high-level metrics and initiative updates. I also conduct a Global Information Security report that has far more detailed metrics and operational data."

- David Levine, CISO, RICOH (original quote from Feats of Strength, June 2018)