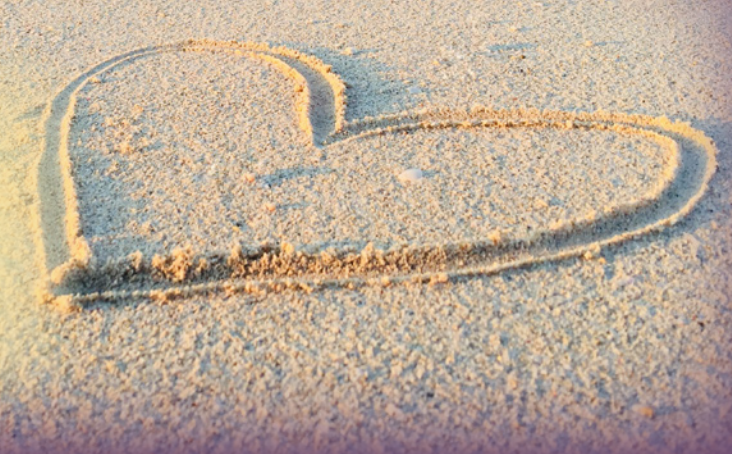
The Five Love Languages

For CISOs and Boards

How to Express Actionable Metrics to Your Stakeholders



"Given a **63%** *probability that an attacker could compromise our defenses in a ransomware attack costing upward of* **$244 million**, *I recommend we spend* **$200K** *on a device to mitigate attacks."*

– CISO

Words of ~~Affirmation~~ *Quantification*

Don't make it all about you by telling the board about your shiny new toys and how you need more. Instead, show them proof that what you're doing is nurturing the organization. Putting cyber risk in financial terms conveys to the board that you not only care about the organization and understand its business goals, but that you're also equipped with the skills to help strengthen its market position.

Quality ~~Time~~ *Metrics*

Pretty pictures only go so far. If you throw a dizzying amount of numbers and graphs at the board, not only could they garner no meaning from your presentation, but they may also wonder if you're hiding something. Make sure the metrics you present are meaningful and ring true by presenting only the numbers that showcase the effectiveness and ROI of your security program.

Receiving ~~Gifts~~ *Gifs*

Kidding! Boards don't care about GIFs. What they do care about are strategic business objectives. To understand those objectives, take the time to get to know the board. What experiences led them to serve your organization? Build trust by asking them directly about their top business priorities and goals. Then describe how your security efforts help achieve those goals.

Acts of ~~Service~~ *Security*

It's not what you can ***get***, but what you can ***give***. Reducing cyber risk isn't just about your professional success (although that's a probable outcome), and it's not even just about defending the organization (though that's also key to a strong relationship with your board). When you look deeply, you will see that defending against cyberattacks protects the people whose data you've promised to safeguard. Make sure the board knows that you take that vow seriously and intend to honor it.

Physical ~~Touch~~ *Tangible Proof*

Don't touch the board. That said, some things do need to be tangible, like the ROI of your cyber stack. The average security team uses 47+ different products, but 53% of enterprises don't know if their security tools even work.* While a layered defense is good, ineffectual or excessively duplicative solutions waste precious resources. Be able to talk about the percentage by which your spend reduces risk, and how much money it is likely to save.

Communicating in a language your board understands will enrich your relationship and the depth of your collaboration, justifying budget and strengthening your security program. Since an effective security program not only reduces the risk of a costly breach, but also builds trust with customers and partners, it enables the growth of the organization itself.

FOR MORE ON HOW TO QUANTIFY CYBER RISK AND ALIGN WITH YOUR BOARD, VISIT

securityscorecard.com/board-common-ground

* https://www.helpnetsecurity.com/2019/07/31/are-security-tools-working/

SecurityScorecard