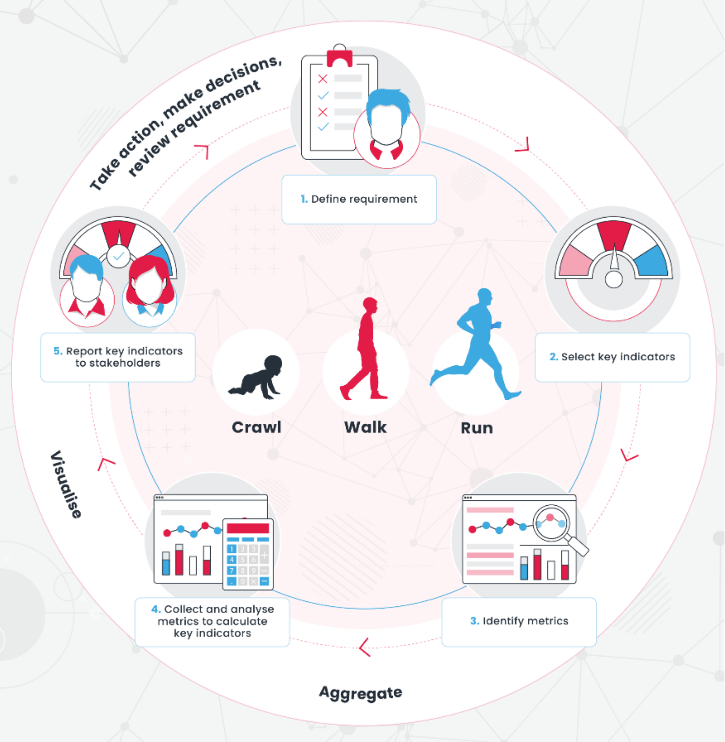
Navigating the politics of measuring security

Treading a fine line between candour and practicality

One of key recommendations from our research into Measuring Security was that measurements must provide clear insight that supports decisions and/or drives action. We outlined a measurement cycle that helps maintain communication with decision-making stakeholders, keeping their requirements up-to-date and improving the organisation's ability to measure information risk and security performance over time (see the graphic on the right). But what happens when those decision-makers simply don't want to hear what the data has to say? There is a moral and ethical maze to navigate, in addition to the work of actually measuring security.


Take action, make decisions, review requirement
1. Define requirement
2. Select key indicators
3. Identify metrics
4. Collect and analyse metrics to calculate key indicators
5. Report key indicators to stakeholders
Crawl
Walk
Run
Visualise
Aggregate

Security leaders often find themselves in a precarious position when navigating boardroom politics in organisations where information risk management is not always a priority. They can't go in all guns blazing with a fully honest account of how poorly the organisation's security posture is – they may even be under pressure to obfuscate or omit certain details. However, presenting a watered-down version of the truth is likely to come back to bite them later when an incident occurs and questions start flying about who knew what, and when.

Antagonising people to the extent that they don't ask for further security status reports – or simply switch off whenever a security practitioner enters the room – is counterproductive to helping the organisation manage risk. A mix of soft skills is needed to complement the message being conveyed, and there is a fine line to tread between speaking truth to power and saying just enough to have an influence.

Why presenting the full truth around security measurements can be difficult

It is often the case from a security posture perspective that the better you measure, the worse you will look. This is, of course, simply a case of changing perceptions: the level of risk remains the same as before those measurements were taken; that risk has now been exposed and it can be dealt with. However, presenting decreased performance (or previously unknown poor performance) can be a shock to the system, and communicating that change can be fraught with difficulty.

Speaking truth to power doesn't always go down well: some may take bad news as a personal slight, or don't want to know the full extent of a risk if it relates to their own areas of responsibility and reflects on their performance. Some want plausible deniability when things go wrong. Others may want to cook the books to make everything look fine, when they know that performance is not what it should be.

"I've had several conversations where the executive I was reporting into wanted to lower reporting thresholds so that a sea of amber would turn green." – ISF Member

Board members are often used to thinking they know and understand everything about their business: if something comes up that they don't understand, some have the reaction of shying away from, or flat-out denying it. They don't want to ask questions for fear of looking unknowledgeable, nor do they appreciate surprises. Such a culture can have a detrimental impact if it leads to security reporting going unchallenged or misunderstood.

As a result of these challenges, some security leaders fall into the trap of viewing board reporting as a chore that needs to be survived: walking in, dazzling the audience with death by PowerPoint, reporting a range of figures in the hope that their meaning won't be questioned, and exiting while paying lip-service to some basic actions. The chore is repeated every six months. But this ensures that meaningful engagement or change never occurs.

Establishing rapport: relationship-building is essential

The work of making board reporting easier starts outside the boardroom. Security leaders should aim to build relationships beyond that formal setting, enabling private conversations where decision-makers can ask questions and build up their own level of understanding without fear of embarrassment in front of their peers. Having had this opportunity, such decision-makers may even act as cheerleaders for security.

Security leaders are likely to find it useful to build relationships beyond their direct line of reporting, particularly in cases where the person that the security leader reports into (e.g. the CIO or CFO) is not interested in relevant and accurate security reporting and wants to keep things in siloes.

It's a tricky path to navigate if your boss is part of the problem, but without necessarily going over their head, it is possible to establish relationships with other executives so that they are comfortable to come to security with questions or concerns. Building these relationships can also have the additional benefit of raising the profile of security throughout the business.

To help build relationships and get on an equal footing, security leaders need to find out what most concerns executives, and find common ground: how can security address those concerns? Language is also key: while always tempting, it's important to avoid jargon and coming across as a technical know-it-all: security leaders have to find ways to speak directly and clearly in terms that make sense to the audience as well as making sure they listen to what the business is saying.

Security leaders should also carefully pick their battles. This can mean starting slow and drip-feeding basic information about security performance, even when you know there is a major transformation required. It can take time to get others up to speed or to understand the scale of an issue. Going into great detail around numerous risks or threats can be off-putting or lead to lack of understanding. It can also give a sense of being overwhelmed. So, it may often be better to hold back, if reporting everything you know is going to be counterproductive.

Of course, not reporting everything you know comes with its own hazards, especially if and when one of those identified but unreported risks rears its head. Security leaders should set out a strategy for improvement as soon as possible so that if something happens that was a known possibility, they can show how it could be dealt with as part of the pre-existing strategy.

Putting yourself in a position to ask the right questions and provide useful answers

In the end, measuring security is about supporting the business, helping it to understand the particular challenges and threats it faces and the extent to which it is prepared to deal with those challenges. It is all well and good knowing how well or poorly the organisation is protected; that knowledge is only useful if it actually leads to action. Security leaders and practitioners have to make themselves heard, whilst also recognising that it can be better to listen at times. This does not mean shouting loud warnings when things aren't perfect, but requires understanding and balance, comprehension of business needs, and a knack for relating to individuals. Classic soft skills must go alongside diligence, technical know-how and analytical thinking.

To make a difference, security leaders need to be able to communicate well with the relevant and important people, when it matters. Asking the right questions and demonstrating how you can bring value can turn into a self-perpetuating cycle: the more you prove you can help, the more likely you are to get into meaningful conversations at the next meeting, the more forthcoming decision-makers might be about their requirements, and the better they become at asking meaningful questions about security.

"If you just ask executives 'what do you want to know?', you get static questions such as 'are we secure?' Often, many execs don't really want to be involved in those discussions. But if we start slow, we can test the waters and then gradually educate." – ISF Member

It is a well-rehearsed trope that culture change is required to enable honest and productive conversations around security. This is often true, and culture is indeed driven from the top, so it is not something that security leaders can make happen on their own. One key required shift in organisational culture would be to rely less on strict hierarchy and communication chains: people at different levels of the business should be able to exchange ideas and highlight issues. This is an area where security leaders can help to drive change, by being proactive in discovering the needs of the business and key individuals. Security leaders can position themselves and their teams as indispensable, critical friends to decision-makers.

Richard Absalom is a Principal Research Analyst at the Information Security Forum.

Richard Absalom – Information Security Forum

richard.absalom@securityforum.org

February 2023