securityweek.com

CISOs and the Quest for Cybersecurity Metrics Fit for Business

Tags: NEWS & INDUSTRY Risk Management Management & Strategy

19-25 minutes

Never-ending breaches, ever-increasing regulations, and the potential effect of brand damage on profits has made cybersecurity a mainstream board-level issue. It has never been more important for cybersecurity controls and processes to be in line with business priorities.

A recent survey by security firm Varonis highlights that business and security are not fully aligned; and while security teams feel they

are being heard, business leaders admit they aren't listening.

The problem is well-known: security and business speak different languages. Since security is the poor relation of the two, the onus is absolutely on security to drive the conversation in business terms. When both sides are speaking the same language, aligning security controls with business priorities will be much easier.

Well-presented metrics are the common factor understood by both sides and could be used as the primary driver in this alignment. The reality, however, is this isn’t always happening

Using metrics to align Security and Business

SecurityWeek spoke to several past and present CISOs to better understand the use of metrics to communicate with business leaders: why metrics are necessary; how they can be improved; what are the problems; and what is the prize?

Demolishing the Tower of Babel

“While some Board members may be aware of what firewalls are,” comments John Masserini: CISO at Millicom Telecommunications, “the vast majority have no understanding what IDS/IPS, SIEMs, Proxies, or any other solution you have actually do. They only care about the level of risk in the company.”

CISOs, on the other hand, understand risk but do not necessarily understand which parts of the business are at most risk at any time. Similarly, business leaders do not understand how changing cybersecurity threats impact specific business risks.

The initial onus is on the security lead to better understand the business side of the organization to be able to deliver meaningful risk management metrics that business leaders understand. This

can be used to start the process for each side to learn more about the other. Business will begin to see how security reduces risk, and will begin to specify other areas that need more specific protection.

The key and most common difficulty is in finding and presenting the initial metrics to get the ball rolling. This is where the different ‘languages’ get in the way. “The IT department led by the CIO typically must maintain uptime for critical systems and support transformation initiatives that improve the technology used by the business to complete its mission,” explains Keyaan Williams, CEO at CLASS-LLC. “The Security department led by the CISO typically must maintain confidentiality, integrity, and availability of data and information stored, processed, or transmitted by the organization. These departments and these leaders tend to provide metrics that focus on their tactical duties rather than business drivers that concern the board/C-suite.”

Drew Koenig, consultant and host of the Security in Five podcast, sees the same basic problem. “In security there tends to be a focus on the technical metrics. Logins, blocked traffic, transaction counts, etc... but most do not map back to business objectives or are explained in a format business leaders can understand or care about. Good metrics need to be tied to dollars, business efficiency shown through time improvements, and able to show trending patterns of security effectiveness as it relates to the business. That's the real challenge.”

Williams sees the problem emanating from a lack of basic business training in the academic curriculum that supports IT and security degrees. “The top management tool in 2017 was strategic planning,” he said. “Strategic planning is often listed as one of the top-five tools of business leaders. How many security leaders

understand strategic planning and execution enough to ensure their metrics contribute to the strategic initiatives of the organization?"

It is not up to the business leaders to learn about security. "The downfall for many CISOs in the past is believing that business needs to understand security," adds Candy Alexander, a virtual CISO and president-elect of ISSA. "That is a mistake, because security is our job. We need to better understand the business, so that we can articulate the impact of not applying appropriate safeguards. The key to this whole approach is for the CISO to understand the business, and to understand the mission and goals of the business."

Is it worth the effort?

With no exception, the CISOs *SecurityWeek* spoke to believe that better presentation of the right security metrics will help align security and business. In fact, comments Alexander, "It is the only way CISOs can get executive management to understand what the challenges are and what the successes have been."

That doesn't make it any easier. Apart from metrics and the security /business dynamic, CISOs must also understand the psychology of the boardroom – and that will vary from company to company. "Some boards care greatly about security, and others have little interest," comments Daniel Miessler, director of client advisory services at IOActive. "If, for example, the business is being crushed by a competitor, having nothing to do with security, then it could be (but not always) that security is justifiably a lower priority to the board."

Timing thus becomes an issue over which the CISO may have little control. Should metrics presentations be regular or given only when

necessary. The former may unnecessarily take up the business leaders' time, while the latter will paint the CISO as the bringer of doom.

Tomas Honzak, CISO at GoodData, feels that reporting should be rare. "The board should not be hearing about security on a regular basis," he told SecurityWeek. "Unless there is a critical issue or significant business transformation, an annual presentation of the key trends, evolution of the threat landscape and strategic security plans are all that the board should be receiving from security."

This is a minority view. Many CISOs at least imply that metrics reporting should be delivered sufficiently frequently to be able to show trends.

And then there's style. Having got the opportunity to present to business leaders, it is very important that it is not wasted. "Many reports are like some presenters – single toned and boring," comments Steven Lentz, head of security at Mojio and former CSO at Samsung Research America. "The report is either too long (too much detail) or too much fluff. If the report is not good it will simply cause more questions to be asked."

The solution, he suggests, is that CISOs need be a sales and marketers as well as a security experts. The presentation itself must be like a good CV, able to capture attention within the first few sentences and maintain interest through the duration. Critically, he adds, "The report will answer questions rather than having the board question the report."

This is key and strikes at the very core of metrics reporting. If the purpose is to say, 'look how good your security team is', or to highlight a new problem that needs more budget, then you should

expect queries. But if the purpose is to align your security with business priorities then the metrics need to be more self-explanatory. They can be provocative, to provoke comment and discussion with and from the business leaders, but they should not elicit queries on the reporting itself.

Are CISOs delivering adequate metrics to the board?

Asked if CISOs are currently delivering good metrics, the answer was an unequivocal yes and no, maybe, it depends, but probably not.

Metrics reporting is a classic chicken and egg problem. To deliver good metrics, the CISO must understand what the business leaders want; but understanding this want comes through aligning security and business through delivering effective security metrics.

Ideally, the CISO should already be at the level of the C-Suite. “A critical enabler delivering business-centric metrics is that the security function is not simply reporting up into the C-suite but is instead being part of that level,” suggests Raef Meeuwisse, a CISO consultant and author of Cybersecurity for Beginners. “Only where security is engaged and involved in the highest levels of the business can any organization hope that their security approach, including what is measured and reported, will reflect a deep understanding of the business strategy, direction and needs.”

That, sadly, is rarely possible. “Unfortunately, the governance crisis continues,” explains Tom Kellermann. chief cybersecurity officer at Carbon Black, “as most CISOs still report to CIOs. Your defensive coordinator is reporting to your offensive coordinator.” What the CIO is often most interested in learning (how often security has prevented downtime) is not the same as what security should be

reporting to business (such as how, why, and by how long dwell time has been reduced).

Poor metrics is more common than no metrics. “For example, I see many security programs that report on the number of threats blocked by security tools because the logs are easy to parse. It is a bonus that the volume of blocked threats sounds impressive. Unfortunately, this data rarely informs the business decisions that concern the board/C-suite.”

Do vendors help with producing metrics from their applications?

It would help if vendors produced readymade presentable metrics as part of their application reporting capabilities. Some are trying. “With a resurgence of interest in quantifying one’s security posture, vendors are looking more to provide this across different parts of the hybrid infrastructure,” explains Anupam Sahai, VP of product management at Cavirin. “This is also a major initiative by service providers and MSSPs. The Verizon Risk Report is a good example.”

Not all vendors agree. “This is not a vendor issue,” said Chris Morales, head of security analytics at Vectra.

“The issue is whether or not there is solid alignment between the metrics that security wishes or needs to use and the information that the board requires,” explains Steve Durbin, MD of the Information Security Forum. His concern is that applications usually generate a high volume of detailed statistics that require significant processing (normalization, aggregation and analysis) before they can be interpreted and presented to the board.

The metrics presented to the board, he continued, “should convey details relating to targets of particular interest to each audience, and be clear, concise and limited in number (often four or five).”

Chris Key, CEO and co-founder of Verodin, goes further. “Relying on a vendor to provide meaningful metrics on the effectiveness of the control they sold you is like having the fox watch the hen house. Additionally, no single vendor's control represents the effectiveness of an organization’s full cybersecurity strategy.”

Less bluntly, Meeuwisse explains, “Vendors have a tough time because they are usually being squeezed on price, often asked for their security metrics in a different format for each customer and can be trying to achieve security on a smaller budget than many of their customers. As someone who has audited tens of different

suppliers in my time, I almost always find substantial gaps. Most vendors show an increasing willingness to provide security metrics, but my own experience is those metrics, when available, are usually carefully crafted to avoid displaying any real issues."

"Some vendors require log aggregation to a separate reporting server running its own analytics software, which can be an expensive and complex solution," comments Heather Paunet, VP of product management at Untangle. "Additionally, some vendors only offer very high-level, canned reports that don't enable administrators to drill down on specific issues, limiting their usefulness."

For board-level metrics, analytics data must often be combined with some sort of cost-benefit analysis, something that few vendors provide out-of-the-box. "It's important," she suggests, "that security teams select vendors who provide database-driven reporting that can be easily customized to fit their needs."

The consensus is that vendors can and should provide raw data on their product performance, but the CISO will always need to collect, correlate, analyze and present the right metrics in the right form in a manner that directly relates to the interests and concerns of business leadership.

What makes a good metric?

This all begs the question: what makes good metrics that are relevant to business leaders and can be used to further the alignment of security and business?

"Transforming security metrics into business information requires a change in focus and reporting format," claims Williams. "Businesses measure progress and performance using scorecards,

monthly or quarterly business reviews, and KPIs. Any security metrics provided to the business need to contribute to the performance measures that the business is already conducting. Providing security information that answers business questions is far superior to providing technical information and log details that have no relationship to business goals and objectives."

"I like the old cliché that metrics need to be SMART – Specific, Measurable, Accurate, Reliable and Timely," suggests Martin Zinaich, information security officer at the City of Tampa, Florida. "If done properly metrics can help align the Security Office to the Business and vice versa."

He likes to keep things simple but informative. "Using standard Red/Yellow/Green indicators can quickly show the board alignment to risk, compliance and governance. Graphs can be leveraged to show risk reduction over time and overall framework alignment. Quad charts can quickly show top risks, issues requiring management attention, any major incidents and relevant projects in-flight. The goal is to be informative but brief, not technical, but statistical and aligned for a business/infosec synergic relationship."

Sahai agrees that simple is best. "Consider the FICO score," he says. "So, a single metric, say on a scale of 0 (worst) to 100 (best), that reflects a combination of the organization's security and compliance posture." The devil, of course, is in the detail. "If you look at how hackers infiltrate and compromise an organization, a score may be developed using the same approach. You first discover and classify resources, both on-prem and in the cloud, and assess threats against them, both internal and external. Based on this assessment, you identify any weaknesses and then evaluate the resources against any controls in place."

The result, he continued, “is an overall score that reflects the organization’s current cyber posture. Correcting identified weaknesses will raise the score. Additional elements that go into scoring may include the likelihood of the breach and the projected impact. This latter point can map to the CIA model – confidentiality, integrity, and availability.”

Trends are important. “Can you provide month-over-month statistics of how each business unit has reduced the inherent risk across the company because the average time to patch has decreased significantly?” asks Masserini. “Those are the types of metrics the Board cares about, not how many attacks the firewall blocked, or how many patches are missing across the entire infrastructure, or any other ‘frighten them with huge numbers’ type metrics.”

Those huge numbers may be relevant to infosec at the operational level, says Bonney. But, he adds, “At the board level, it’s fundamentally speaking the board’s language – the board has a fiduciary duty to protect the business and keep it a going and growing concern. Align the metrics you report to the board with these goals. Deliver the metrics in terms they understand – impact on the business not impact on or of the technology – and make sure they know what the ask is. Never leave a board meeting without making the ask.”

Lentz also agrees that reporting must be continuous, with trends rather than static points in time. “I believe you also need to do a trend report,” he said. “In other words, over time – say month to month – showing a year. This way the board can clearly see wins, improvements, and areas of concern that need addressing. A clear visual presentation and roadmap so the board can grasp rather than look confused.”

Morales goes deeper and offers specific metrics to include: dwell time, lateral movement, reinfection, network coverage and response time.

Miessler and Kellermann show how these issues can be combined and worked into business-centric metrics.

“Two that we really like to include,” said Miessler, “are firstly, the amount of risk visibility present in the organization (percentage of systems under security management). That is, don’t just report on what you can see, but what percentage of risk isn’t yet visible to you because of technological and time limitations. Secondly, the percentage of systems under management that have x, y, and z level of defenses implemented. These are quite different, as you can have great numbers for the latter while having bad numbers for the former, and risk will still be very high.”

Kellermann proposes “three grades of measurement which are encompassed in the level of risk posed to the information supply chain and operations for a company. These begin with the results from hunt teams to discern if there is a current compromise and what is the scale? Second how quickly can that cybercrime be suppressed and contained? Lastly, are we compliant with the security standards mandated in our industry and our geography. If not, why?”

Like Sahai, Paunet believes the different metrics should be brought together to show the overall security posture of the organization. “It's also helpful to show how the threat landscape and an organization's response is changing over time. This gives the executive team, who may not be cybersecurity experts, some insight into why security is business-critical and worthy of continued

investment. CISOs need to distill security insights into something that can be consumed by a non-technical audience that is more interested in the ‘why’ than the ‘what’.”

Meeuwisse warns against being totally insular. “What technology and threat changes are being anticipated or experienced elsewhere in your industry? A dashboard about emerging threats is a great way to check if everything appears to be in hand and if anything needs to be added for consideration.”

But in the final analysis, as Chris Key succinctly says, “The best metrics demonstrate how effective the cybersecurity program is at achieving key business objectives.”

The key takeaways

What is clear from these discussions is that there is no simple answer to what makes good infosec metrics for reporting to business leadership. The detail will vary from industry sector to industry sector, and even company to company, depending on the key business drivers.

It is equally clear infosec must understand business. CISOs cannot expect business leaders to understand security. The purpose of the metrics is to explain how security supports, or could further support, business priorities. To do this, CISOs must understand those business priorities.

The problem here is that such understanding comes best from being a part of the overall business leadership – which rarely happens. In a few enlightened cases, CISOs have at least a voice at the board; but in most cases they still report to the CIO who will have his or her own priorities sometimes at odds with the CISO’s priorities.

Cracking the metrics nut is important. The prize is high – nothing less than more efficient security, a more profitable business, a greater likelihood of gaining budget when it is required, and greater personal visibility at board level. When security is seen to provide protection at the right level and in the important places, it genuinely becomes the enabler of safe business and increased profits rather than a simple drain on corporate funds.

Without good metrics, security and business alignment is unlikely. And without that alignment, security will be patchy and business at risk.

Related: Report Depicts Shameful State of Cybersecurity Metrics

Related: The Art of Measuring Security Success

Related: Why Business Has a Problem With Security Metrics

Related: Establishing Your Own Metrics: What Not to Do

Related: Using Relative Metrics to Measure Security Program Success

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend: