www.KennaSecurity.com

WHITEPAPER

Reporting on Risk to the Board: A CISO's Approach

When I ran security at Orbitz, reporting on risk was always a challenge. My team wanted to ensure that we had a clear way to paint a picture of the organization's exposure to risk—as well as describe the actions we had taken, month by month, in order to reduce it.

But frankly, we weren't very good at it. We could only use the tools we had available to us, and those tools didn't equip us with a sufficient ability to see, measure, and monitor our risk landscape. We could only do one thing really well: play the numbers game. In other words, we were really good at reporting on the sheer volume of issues we addressed.

Fast forward several years and I can see that little has changed. When I talk to companies prior to their joining the Kenna Security platform, I find that reporting on vulns closed—rather than taking a more strategic view of risk—is still the primary modus operandi.

In this article, we'll take a look at why this approach fails—and how it may be possible to swap out the "numbers game" with a more comprehensive view of risk. I'll explain conceptually how you can do that. Of course, I'll also talk about how Kenna can help, but my intention is to help inform your approach even if you have no interest in Kenna.

How Reporting is Being Done Today

In many organizations, reporting on risk is actually all about volume: “We closed this many vulns last quarter, and last month, and this month.” Sometimes, the extra step has been taken of assigning CVSS or scanner scores to each vulnerability, with the hopes of demonstrating that the closed vulns represent a particular level of criticality.

Here’s a couple of examples of the types of reporting we see all the time. While these examples are generic they represent the same types of metrics we see time and time again. The reality is, these examples could come from any of several hundred thousand companies, because most organizations are reporting on risk in the same way.

Example #1

Assets	Vulns	% of Asset Reporting Vuls	Average Days open	Unique Vulns	CVSS Risk Level
EXTERNAL - PCI	222	38%	163	24	Level 1
EXTERNAL - PUBLIC	300	34.00%	34	99	Level 3
APACHE	53	97.33%	455	5	Level 4
AWS	85	80.90%	82	123	Level 4
CASSANDRA	313	61.67%	192	43	Level 4
BASTION	4313	95.19%	4819	234	Level 2
NETWORK	4314	100.00%	54	111	Level 4
BOSS	233	56.82%	124	56	Level 4
TOMCAT	452	23.33%	689	65	Level 4
QUICKTIME	57	89.77%	78	3	Level 1

Example #2

Summary

All Active Vulnerabilities						Total #	Closed since June 1	*Past Due Vulns Since May 21		
External		DMZ		Internal						
Exploitable	Non-Exploitable	Exploitable	Non-Exploitable	Exploitable	Non-Exploitable			External	DMZ	Internal
34	83	8203	5800	20912	61944	97242	7377	⇧ 45	⇧ 3211	⇧ 54181

SOX

All Active Vulnerabilities						Total #	Closed since June 1	*Past Due Vulns Since May 21		
External		DMZ		Internal						
Exploitable	Non-Exploitable	Exploitable	Non-Exploitable	Exploitable	Non-Exploitable			External	DMZ	Internal
2	5	631	843	2911	3628	7315	1112	⇧ 12	⇧ 32	⇧ 1523

PCI

All Active Vulnerabilities						Total #	Closed since June 1	*Past Due Vulns Since May 21		
External		DMZ		Internal						
Exploitable	Non-Exploitable	Exploitable	Non-Exploitable	Exploitable	Non-Exploitable			External	DMZ	Internal
0	0	613	480	6042	9021	24267	1244	⇧ 0	⇧ 311	⇧ 6134

Each of these examples shows a highly ordered, professional approach to vulnerability management. They group the assets appropriately, assign levels of risk to them, and sort them by orders of severity. Some of the metrics include scanner coverage, vulnerability density, and time-to-remediation metrics.

Here's the problem: they're completely useless for understanding the organization's true exposure to risk. These spreadsheets represent an inventory of vulnerabilities, and indicate some level of prioritization assigned to them according to CVSS, but there's no true context.

Any member of the board will scratch their head and ask, "Great, you closed 10,000 vulnerabilities last month. So...is that... good?"

Then they will proceed to ask:

- **What's our true risk level now, and where was it before?**
- **Where is it in relation to where we need it to be?**
- **What's our progress been over time—not in simply closing vulnerabilities, but in reducing our exposure to risk?**

None of these questions are answered in these intricate and well-meaning spreadsheets. They demonstrate a mastery of vulnerability volumes, but not an ability to understand the organization's actual risk posture.

Any member of the board will scratch their head and ask, "Great, you closed 10,000 vulnerabilities last month. ***So...is that...good?****"*

What the Board Really Wants to Know

Closing vulns and scoring with CVSS does not answer the questions that the board truly wants to know:

- **What's our likelihood of a breach?**
- **If we have a breach, what's the impact?**
- **What assets are most exposed, and what's the plan for reducing that exposure over time?**
- **What's the cost for that reduction, and does it align with the current allocation of budget and resources?**

Any board will want storytelling behind the data. They don't just want a static number—but rather a narrative that aligns all the pieces of the organization's security landscape and describes its overall progress towards reducing risk.

Let's talk about how to actually do that.

One Metric to Bind Them All

Your first step is to understand the criticality of your various asset inventories. For example, you may know that a particular asset contains all of your highly sensitive customer data—whereas another asset group is a set of workstations containing no sensitive information or critical information or processes. If both of those assets have the same likelihood of a breach, you want to focus on the one with the most impact to the business, and prioritize the vulnerabilities in that environment first.

Once you have completed arranging your environment to represent some degree of importance and potential impact to the business, the real work begins: you need a true metric to measure risk. As I'm sure is clear by now, reporting on the number of closed vulns is the wrong metric to choose.

What you need to do is bring together your assets with external intelligence on what's happening "in the wild"—in other words, what activity poses a threat to your organization right now. Whether it's poor password policies, misconfiguration issues, or critical vulnerabilities that are actively being exploited either through advanced threats or targets of opportunity, it's this real-time context that suddenly turns a simple number into a story that even a layman can understand.

Additionally you'll want to know what if any compensating controls exist around your weaknesses. Perhaps there's a weak password policy in place on a system that when you take a step back is covered under two factor authentication.

Next, you need to be able to report on this metric repeatedly and consistently—over and over again—day to day, month to month, quarter to quarter. Whether the trend line goes up or down, you'll be able to mark your progress to goals.

Asset State + External Intelligence = Trend Line

The metric needs to be simple, understandable, and repeatable, showing historical trends:

- **Here's where we are**
- **Here's where we're going**
- **Here's how we're getting there**

How Kenna Can Help

Ok, you knew it was coming... If you take into account the general concepts I've discussed, you can create the reporting you need without Kenna. But modestly, I think I can safely say that doing so will create a lot of work for the team.

Kenna automates a lot of the steps we've discussed: it takes into account assets, context and external threat intelligence, and part of the platform's functionality is to create a trend line of risk—superimposed against vulnerabilities, just in case you can't live without that number—so you're able to track your progress over time, and create a report that is truly board-ready.

Here's a sample of our reporting screenshot:

A lot simpler to look at than the spreadsheet reports we looked at earlier, right? While what we're looking at here is the "Kenna Score"—which combines both assets with external threat intelligence—it does serve the purpose of providing a simple, understandable metric. And reporting on risk versus vulnerability count can be quite powerful: imagine having the conversation where you explain that vulnerability counts are going up, but overall risk is going down—since the team is remediating the vulnerabilities that truly present risk to the business, rather than a mountain of non-critical vulnerabilities that actually pose no threat. Such a non-intuitive trend line is quite possible if your yardstick is risk rather than the usual numbers game.

At Kenna, we find that presenting a trend line of risk sparks important conversations. People begin to understand the company's past trajectory and future path. And it becomes much easier to discuss budget allocations to help support critical aspects of the business that still may be exposed to risk.

Summary

Forward-thinking organizations can begin to move away from simply assessing vulnerabilities and move towards an approach where you're evaluating exposure to risk, rather than counting beans (or vulnerabilities, as the case may be). The appropriate arranging of assets, an integration of those assets with external threat intelligence, and a clear, simple reporting metric can all be used to paint a picture of risk than even the most non-technical person on your board can easily understand.

About Ed Bellis & Kenna Security

Ed Bellis is the Cofounder of Kenna Security, a SaaS platform that correlates external Internet breach data, exploit data and zero-day threat intelligence with internal vulnerability scan data so organizations can focus on fixing the most critical vulnerabilities. Kenna processes over a billion vulnerabilities a day against Internet breach data for its users.

Ed formerly served as the CISO of Orbitz, where he built and led the information security program and personnel for over six years. Ed has over 20 years of experience in information security and technology and is a frequent speaker and contributor to the information security community.

For more vulnerability management best practices:
visit www.kennasecurity.com