SCTE CABLE-TEC EXPO 23
CELEBRATING 40 YEARS

2023 Fall Technical Forum
SCTE • CABLELABS • NCTA

Motivational Metrics for Security

Driving Progress Without Burning Bridges

Matt Carothers
Senior Principal Security Architect
Cox Communications
6305 Peachtree-Dunwoody Rd, Atlanta, GA 30338
+1 (404) 269-7220
matt.carothers@cox.com

Brad Boucher
Vice President and Deputy Chief Information Security Officer
Cox Communications
6305 Peachtree-Dunwoody Rd, Atlanta, GA 30338
+1 (404) 269-8880
brad.boucher@cox.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

1. Introduction

In the modern workplace, cybersecurity teams operate in matrixed organizations. Security teams drive and track progress without direct authority over developers, system administrators, and other employees responsible for implementing security policies. Many people focus narrowly on the measurements themselves without considering the impact they have on those being measured. This leads to ineffective systems that make employees feel scrutinized and punished.

This paper discusses techniques for designing metrics that not only measure security in a meaningful way but also address the human element. It takes you on a journey through our security program, tells you what we learned from the mistakes we made along the way, and leaves you positioned for success.

Why is it so Hard to Measure and Report on Cybersecurity?

Cybersecurity measurement, metrics, and reporting are still in their infancy. As a comparison, consider the accounting industry and associated financial reporting norms and regulations. We take for granted that we can compare the financial health of companies through standardized balance sheets, income statements and cash flow statements. Building on those financial statements, finance professionals use ratios such as earnings per share and return on invested capital as key financial metrics to quickly compare companies and assess their relative performance or overall financial health.

Entities like the Financial Accounting Standards Board (FASB) and the Securities and Exchange Commission (SEC) developed those practices over the course of nearly 100 years following the stock market crash of 1929 and the subsequent Great Depression. In comparison, control frameworks like the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) are still relatively early in their lifecycles, so we must give ourselves (and the teams we are trying to measure) a little grace and remember that we are still in the early stages of this journey.

2. Metrics Literacy

Even once we determine what needs to be measured, we often do so in a way that makes no sense and yields bad results. Not all mathematical operations apply to all measurements. Using operations like multiplication and division on scales that do not support them leads to bad decision making. To understand why, we need to take a moment to discuss the four types of measurements.

2.1. Nominal

Nominal measurements express set membership. They can be taken by asking simple yes-or-no questions. For example, by asking “Is EDR installed on this server?” for every server in our environment, we create a count of servers belonging to the set with EDR.

2.2. Ordinal

An ordinal measurement tells us one thing is greater than another, but not by how much. For example, let’s consider movie ratings. We can say a five-star movie is better than a one-star movie, but we cannot say by how much. Is a five-star movie five times better than a one-star movie? Will we get the same enjoyment from watching five one-star movies as we would from one five-star? Likely not.

In the cybersecurity world, the Common Vulnerability Scoring System (CVSS) serves as a great example of an ordinal scale. A CVSS score of 10 is more severe than a score of 5, but we cannot say it is exactly

twice as bad. Nor could we ever say with a straight face that 10 vulnerabilities with a CVSS score of 1 are just as bad as a single vulnerability with a score of 10. Beware of scoring systems that add, subtract, multiply, or divide CVSS scores!

2.3. Interval

Interval measurements allow us to not only compare two values, but to add and subtract them. The Celsius temperature scale provides a good example. The difference between 10 degrees and 20 degrees is the same as the difference between 90 degrees and 100 degrees. Take care, however, because multiplication does not work on interval scales. 20 degrees is not twice as hot as 10 degrees on the Celsius scale because on that scale the zero point does not mean "no heat." Rather, it is arbitrarily set at the freezing point of water.

2.4. Ratio

Ratio measurements allow us to use not only addition and subtraction, but also multiplication and division. Take mass, for example. 20 kilograms is exactly twice as much as 10 kilograms. This is because zero kilograms means "no mass." The same is true for the Kelvin temperature scale, where zero means "no heat."

3. Setting Goals

Now that we have a good grasp on the math, let us talk about the people. It is a rare information security organization with the authority to simply dictate what must be done. Instead, cybersecurity leaders must build bridges to other departments within the enterprise and create performance metrics that motivate success.

3.1. Socialize the Goal and Explain the Why

The best way to meet expectations is to set expectations. Cybersecurity is no different. It is imperative to socialize the key objectives of a cybersecurity program to its stakeholders and partners. Cybersecurity frameworks contain hundreds of cybersecurity controls, but they rarely explain why they are needed. Even if they contain risk statements, the risks are typically not expressed in business-friendly terms and offer little context.

When establishing the cybersecurity controls needed in a technology environment, take the extra steps to explain why they are important and how they improve the security posture and health of your organization. In these conversations, create a real dialogue with technology teams. Allow them to ask provocative questions, and provide thoughtful answers, even if it means taking on the occasional homework assignment to clarify the position. Working out challenges to the merits of a control at the beginning of the journey is far easier than at the end. "I never agreed we needed that control anyway" must be avoided, particularly when regular measurements and executive reporting begin.

In the same way that explaining the value of security controls is important, cyber security teams must also take the time to understand the "why" from stakeholders. Other teams may have completely valid reasons for pushing back on security controls, and a one-sided conversation will not convince them. Take the time to understand and appreciate the perspectives of others and winning them over will be much easier.

3.2. Set Goals Collaboratively

Collaborative target setting helps boundary partners appreciate that cybersecurity teams understand that security is just one of many business imperatives. A team that helps set its own targets, especially when they feel that competing priorities were heard and thoughtfully considered, will be much more amenable to meeting those targets. For example, the rollout of a new security tool might interrupt the launch of a critical new service. Identifying this conflict early is always better than in the middle of a struggling implementation.

This can certainly be a complex conversation, but the dialogue created in these discussions typically helps both sides learn and build trust. At the end of the day, security organizations want to protect and enable this business, not disable it. Finding the right pace of change and remediation in your organization and culture can help prevent heated battles in the trenches. If the pace of cybersecurity improvement is not moving fast enough, escalate up not down.

3.3. Ensure Partners Understand the Goal Posts Will Move

Security is a continuous process and not a one-time activity. Your partners must be aware that the targets can and will change. If they are not aware from the outset, they will feel increasingly frustrated as it seems their achievements are being snatched away.

For example, say that your security team identifies 1,000 unknown devices on the network and negotiates with the server administration team to document them in an asset management database. The team completes 900 of them, and your measurement shows 90% completion. The next day, your team gains access to another internal tool and discovers an additional 1,000 unknown assets. Suddenly, the denominator is 2,000 instead of 1,000, and the team is now only at 45%. These types of issues will occur in any sufficiently complex organization, and partners must be prepared to face them.

In these cases, you may even add new metrics or provide additional context on readouts to clearly explain that even though the goal posts moved, significant progress was achieved. Taking the above example further, adding a metric that shows number of assets mapped as well as the number of newly discovered assets during a time period acknowledges both great progress being made and a shift in the end target. Going the extra mile to ensure that positive progress is celebrated while the goal posts are moving is important to keep teams motivated.

3.4. Establish Principles and Guardrails Early to Enable Scale

In alignment conversations, work to establish principles and guardrails that can be referenced later when conflicts arise. An example of a principle or guardrail is, “Our internet facing applications must be free of critical and high-risk coding vulnerabilities.” Note that the statement does not address specific vulnerabilities. Instead, it addresses wide classes of vulnerabilities. It is a simpler concept that more boundary partners can understand and adopt, and it prevents security teams from being bogged down arguing about each specific issue individually down the road.

3.5. Look for Incremental Progress

When establishing these guardrails and principles, one must often take incremental wins instead of immediately swinging for the fence. For example, an organization may not even be willing to entertain estimating the cost of what it would take to patch all vulnerabilities throughout the environment every 30 days. But most organizations would find it immediately more palatable to mandate patching only of critical and high-risk vulnerabilities for internet facing systems every 30 days. In this case, patching

internet facing systems would be a defensible first step in a risk-based approach to improving the organizations cybersecurity posture, while also allowing operations teams to learn what it takes to deliver.

4. Measuring Progress Clearly and Fairly

4.1. Use Data Rather than Words

Qualitative (words) measurements can be subjective and imprecise. False communication can occur when two people believe they agree on something but actually hold different ideas of what words mean. Qualitative measurements also suffer from the issue of range compression. If we break our measurements down into buckets like "low", "medium", and "high" or visualize performance with buckets like "green", "yellow", and "red" we lose the ability to show any progress within a bucket.

For example, let us imagine we have a population of 10,000 servers in a data center, and our goal is to motivate the owners to enter information into an asset database. We create a dashboard with a traffic light. The light is red below 25% compliance, yellow between 25% and 75%, and green above 75%. Due to range compression, the teams performing the work will see no change in the status from the time they complete server 2,501 and server 7,500. Furthermore, as soon as they enter server 7,501, the light turns green, and they have no further motivation to continue.

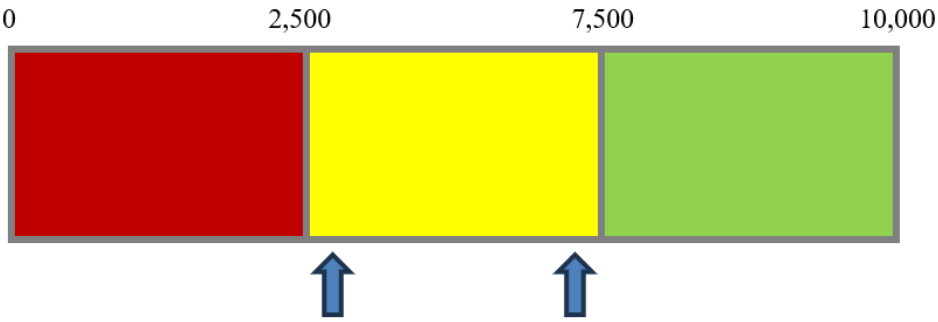

Figure 1 -- Range Compression Hides Progress

4.2. Give Credit Where Credit is Due

Ensure you acknowledge work as it is done. One metric the authors designed internally involved patching compliance. They measured at the application level rather than the device level, so for any given application, multiple devices might need to be addressed. They only counted an application as complete when all associated devices were complete. This created a situation where an administration team could spend weeks updating dozens of servers, but if even one server could not be patched for any reason, the entire application registered as a failure. Understandably, some teams decided that if they could not patch every server for a given application, they may as well not patch any of them. Our Information Technology (IT) partners dubbed it the Brad Punitive Scoring System (BPSS). The authors took the hint and retired the BPSS in favor of measuring devices rather than applications.

5. Communicating Metrics

Simply measuring progress does not suffice if one cannot communicate the results of the measurements in a way that drives change. Here are some things the authors have learned about effective communication in their security journey.

5.1. Show What You Are Not Doing

Another way to ensure our partners understand security is never done is to show them measurements for work that has not started yet or for which we have yet to take any measurements. It sets the stage for later engagements without blind siding them.

5.2. Show Both Magnitude and Velocity

Leaders do not only want to see today's score. They want to know how it compares to yesterday's. They want to understand if the number is going up or down and by how much. As such, dashboards should include not just numbers but the amount of change since the last presentation.

5.3. Know Your Audience

When we make metrics, we typically have at least three views. There is of course a detailed view that provides insight into an exact metric and what is driving the positive or negative score of the metric. We then also create aggregate views for mid-level managers and senior leadership. By creating useful aggregate views upfront, we provide the right level of detail to the right level of leader at the right time. If we are escalating poorly performing metrics, we have polished dashboards or summaries ready to go for leaders to enable them to ask the right questions of their teams and help drive decisions and efforts to get us closer to our desired goals.

The following examples show a hypothetical vulnerability management dashboard with multiple views intended for different audiences. Note that is conveys both measurements and areas where measurements are lacking, and it expresses not only the current values but the rate of change.

5.3.1. Company Wide Application Cyber Metrics

This view is intended for senior technology leadership.

All Application Control Summary

			Visibility				Identity and Access Management						Vuln Mgmt	
Application Categories	# of apps	# of LBs, Servers, Containers	Web Application Firewall		EDR/Logs		Multi-Factor Auth		Priv Access Mgmt		Identity Provider Federation		Patching	
Public Facing	85	3,257	95%	-5	75%	-4	94%	-	86%	-2	59%	+2	74%	+16
Core Services	32	1,267	n/a		80%	+6	88%	+6	93%	+17	n/m		78%	+3
Business Critical	75	6,431	n/a		88%	+5	n/a		88%	+15	n/m		55%	-12
Business Tier 2	250	8,560	n/a		81%	+2	n/a		82%	+6	rba		rba	
Business Tier 3	425	12,654	n/a		83%	+4	n/a		82%	+6	rba		rba	

n/a Control not applicable
n/m Control not yet measured
rba Deprioritized, risk based approach

Figure 2 -- Company Wide Overview

5.3.2. *Filterable Application Cyber Metrics*

This view in intended for various levels of mid-level management. It is the same view as the summary, but filterable by business unit and/or leader.

All Application Control Summary - Filterable by Org and/or Leader

Filter by Business Unit/Organization: Tech Organization 1
Filter by Leader: Leader 1

			Visibility				Identity and Access Management						Vuln Mgmt	
Application Categories	# of apps	# of LBs, Servers, Containers	Web Application Firewall		EDR/Logs		Multi-Factor Auth		Priv Access Mgmt		Identity Provider Federation		Patching	
Public Facing	14	536	100%	-	98%	+6	100%	-	86%	-2	59%	+10	79%	-15
Business Critical	12	1,029	n/a		95%	+5	n/a		89%	+4	n/m		65%	+10
Business Tier 2	74	2,534	n/a		94%	+2	n/a		87%	+3	rba		rba	
Business Tier 3	119	3,543	n/a		83%	+4	n/a		82%	+1	rba		rba	

n/a Control not applicable
n/m Control not yet measured
rba Deprioritized, risk based approach

Figure 3 – High Level View

5.3.3. *Application Specific Metrics at a Glance*

This view moves from categorizing applications into buckets to providing application specific scores and is intended for application owners or managers drilling down to identify problem areas.

Public Facing by Application Summary Drill Down

Filter by Business Unit/Organization: Tech Organization 1 | Filter by Leader: Leader 1 | Filter by Application Category: Public Facing

Application Name	# of LBs, Servers, Containers	Web Application Firewall	EDR/Logs	Multi-Factor Auth	Priv Access Mgmt	Identity Provider Federation	Patching
Application 1	75	100%	98%	100%	89%	100%	98%
Application 2	164	100%	95%	100%	100%	0%	98%
Application 3	45	100%	100%	100%	97%	0%	65%
Application 4	32	100%	100%	100%	98%	100%	45%
Application 5	15	100%	89%	100%	79%	100%	38%

Figure 4 – Mid Level View

5.3.4. Detailed Vulnerabilities for an Application

This view provides the specific vulnerabilities that need to be addressed for an application. This view is meant for operations personnel or developers to act upon.

Aged Vulnerabilities by Host

Compliance	Age	Time Left/Past Due	DNS / Container Image	Environment	Cluster Name	CVE ID	Sev	Title
Non-compliant	181+	1 year past due	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2022-29458	4	ncurses 6.3 before patch 20220416 has an
Non-compliant	181+	1 year past due	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2022-29458	4	ncurses 6.3 before patch 20220416 has an
Non-compliant	181+	7 months past due	app.example.com:4443/exp/coam	Production	eks-exp-dmz-p-1	CVE-2022-42916	4	In curl before 7.86.0, the HSTS check could
Non-compliant	181+	7 months past due	app.example.com:4443/exp/local	Production	eks-exp-dmz-p-1	CVE-2022-42916	4	In curl before 7.86.0, the HSTS check could
Non-compliant	181+	7 months past due	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2022-42916	4	In curl before 7.86.0, the HSTS check could
Non-compliant	181+	7 months past due	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2022-42916	4	In curl before 7.86.0, the HSTS check could
Non-compliant	181+	7 months past due	app.example.com:4443/exp/wirel	Production	eks-exp-dmz-p-1	CVE-2022-42916	4	In curl before 7.86.0, the HSTS check could
Approaching Non-compliant	31-59	2 days left	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2023-1999	4	There exists a use after free/double free in
Approaching Non-compliant	31-59	2 days left	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2023-1999	4	There exists a use after free/double free in
Approaching Non-compliant	31-59	10 days left	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2023-3138	4	A vulnerability was found in libX11. The sec
Approaching Non-compliant	31-59	10 days left	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2023-3138	4	A vulnerability was found in libX11. The sec
Approaching Non-compliant	31-59	10 days left	app.example.com:4443/exp/wirel	Production	eks-exp-dmz-p-1	CVE-2023-3138	4	A vulnerability was found in libX11. The sec
Compliant	31-59	25 days left	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2023-35945	4	Envoy is a cloud-native high-performance e
Compliant	31-59	25 days left	app.example.com:4443/exp/store	Production	eks-exp-dmz-p-1	CVE-2023-35945	4	Envoy is a cloud-native high-performance e
Compliant	31-59	25 days left	app.example.com:4443/exp/wirel	Production	eks-exp-dmz-p-1	CVE-2023-35945	4	Envoy is a cloud-native high-performance e

Figure 5 – Detail View

6. Conclusion

Building a cybersecurity metrics program is a journey. The highest performing security teams establish deep relationships with both business and technology partners based on trust, empathy, and a common commitment to improving cybersecurity in the organization.

When designing a metrics program, it is important to create metrics collaboratively using sound math and ensure those metrics are evaluated fairly. This builds confidence in the metrics and helps stakeholders focus on what makes the metric high or low instead of challenging the metric itself. Metrics should also be tailored for your audience and provide context on both magnitude and velocity. Having the right level of detail for the right audience and showing how metrics are progressing (or not progressing) over time is key to driving productive conversations.

Finally, the most important part of your cybersecurity metrics program is alignment. Alignment on the goals of the program. Alignment that those goals will change over time because technology and attackers are always changing. Alignment that cybersecurity isn't just achieved by cybersecurity and instead achieved by cybersecurity, technology and the business working together. And lastly, alignment that the journey is going take time. It is extremely important to recognize and celebrate the progress that is made incrementally. Each day, each week, each month, you will be improving your security posture and the resilience of your organization.