Making It Count – How To Measure Cybersecurity Success

CoSN Cybersecurity Committee

Introduction

This document is intended to help K-12 information technology teams select, shape, and communicate cybersecurity metrics in a practical, repeatable way. It focuses on how to choose meaningful metrics, tailor them to different audiences, and use them to describe program maturity and progress over time.

Why Cybersecurity Metrics Matter

Cybersecurity metrics are more than numbers on a dashboard, they are tools for understanding, communicating, and improving the district's security posture. When chosen thoughtfully, metrics explain how well the cybersecurity program is performing, describe cybersecurity risks, identify where risks are changing and how security investments support broader organizational goals, and, provide insight into implementation outcomes of policies and procedures.

One of the most important reasons cybersecurity metrics matter is that they support budget requests. Clear, well-chosen metrics help demonstrate:

- Why current investments are necessary to manage risk.
- How past funding has produced measurable improvements.

- What gaps or trends justify future investments.

By connecting metrics to outcomes such as reduced incidents, faster response times, or avoided downtime, organizations can move budget conversations from anecdotal concerns to evidence-based decisions.

Effective metrics help leaders answer critical questions:

- Are our controls reducing risk?
- Are people, processes, and technologies working as intended?
- Where should we invest time, money, or attention next?

When framed as a story, metrics turn technical data into insight that supports decision-making, budgeting, and long-term planning.

What Effective Metrics Reveal

Well-designed cybersecurity metrics reveal patterns, trends, and outcomes rather than isolated data points. At a high level, they can:

- **Demonstrate progress** by showing improvement over time (for example, faster incident response or fewer successful attacks).
- **Expose gaps** by highlighting recurring weaknesses or rising risks.
- **Validate effectiveness** of training, tools, or policy changes.
- **Support accountability** by trying outcomes to specific initiatives or investments.

At a program level, metrics can also help describe cybersecurity maturity, such as:

- Moving from reactive response to proactive detection.
- Shifting from manual processes to automated monitoring and response.
- Demonstrating consistency and repeatability in controls and outcomes.

Over time, trends in metrics can show whether the program is ad hoc, developing, defined, managed, or optimized, without requiring deep technical explanations.

Select Metrics Strategically

Not every available data point needs to be reported. In fact, too many metrics can dilute the message.

Key principles for metric selection include:

- **Don’t give people everything.** Choose a small set of metrics that reinforce your goals and priorities.
- **Support your plan and message.** Each metric should clearly connect to a risk, initiative, or outcome you want stakeholders to understand.
- **Focus on signal over noise.** Metrics should highlight meaningful change, not just activity.

Strategic selection ensures metrics inform action rather than overwhelm the audience.

Use Graphics to Tell the Story

Cybersecurity data is best understood visually. Go low on words and high on visuals whenever possible.

Effective visual approaches include:

- Dashboards that show status at a glance.
- Trend lines that compare "before and after" major initiatives.
- Heat maps that highlight concentrations of risk or vulnerability.
- Simple charts that show proportions, progress, or change over time.

For example, a single chart showing "Mean Time to Detect and Contain Incidents Over Time" can communicate maturity far more effectively than paragraphs of explanation. Visuals help stakeholders quickly grasp what is improving, what is stable, and what needs attention.

Tailoring Metrics to Your Audience

Different audiences need different versions of the same cybersecurity story. The underlying data may be the same, but the framing changes. Please note that some of these recommendations will shift depending on the culture of your organization, for example, the information you share with District or School Leadership may be appropriate for the Board as well

Example: One Endpoint Detection and Response (EDR) Metric, Multiple Audiences

Core metric: Mean Time to Detect and Contain endpoint threats using EDR.

- **Board of Education or Directors**

High-level view: A simple trend graphic showing that average containment time dropped from days to hours over the past year, framed as reduced operational risk and improved resilience.

- **District or School Leadership**

Strategic view: The same metric paired with a short narrative connecting faster containment to reduced downtime, fewer instructional disruptions, and better return on investment.

- **IT and Security Teams**

Operational view: Detailed breakdowns by device type, alert severity, and response method, used to fine-tune processes and automation.

- **Vendors and Partners**

Validation view: Vendor-provided EDR reports showing detection rates, response actions, and coverage levels, used as supporting evidence in broader cybersecurity reporting.

This approach allows one metric to support multiple conversations without creating multiple, disconnected reports.

Clarifying Sources of Metrics

Metrics can come from many sources, including internal systems, assessments, and audits. Vendor reports are a valuable source of possible metrics, particularly for tools such as EDR, email security, firewalls, and vulnerability management platforms.

Vendor-provided dashboards and reports can often be leveraged directly or summarized to:

- Validate tool effectiveness.
- Show coverage and adoption.
- Support trend analysis over time.

The key is to integrate vendor metrics into your broader story, rather than reporting them in isolation.

Examples of Cybersecurity Metrics

Effective metrics align with organizational goals and risk priorities. Common areas include:

- Backup and restore test results.
- Culture as a metric - training, reboots, attitudes based on survey results, leadership signals, culture score.
- Data-loss prevention statistics.
- Endpoint, malware, and antivirus performance.
- Incident response timing and resolution rates.
- Network and firewall activity summaries.
- Penetration testing and audit outcomes.
- Phishing simulation and reporting trends.

Non-technical metrics are equally important:

- Budget spend compared to risk reduction outcomes.
- Cost savings and cost avoidance metrics
- Employee engagement in security training.
- Time to detect and contain incidents.

- Vendor compliance and certification status.

From Bland Metrics to Compelling Stories

Metrics are most powerful when they explain impact.

- **Bland:** "Phishing training completion rate: 85%."

Compelling: Training completion reached 85%. Within three months, reporting of suspicious emails increased by 40%, followed by a 60% drop in phishing emails reaching inboxes after new filtering was deployed, showing the combined effect of people and technology.

- **Bland:** "Firewall blocked 10,000 intrusion attempts last quarter."

Compelling: Automated firewall controls blocked 10,000 intrusion attempts, including a surge during a holiday weekend when staffing was minimal, demonstrating resilience during high-risk periods.

Using Metrics to Describe Program Maturity

When viewed together, metrics can tell a clear maturity story that includes themes such as:

- Consistent reductions in successful attacks suggest effective layered controls.
- Faster detection and containment indicate improving operational capability.
- Increased employee reporting reflects a growing security-aware culture.
- Stable, repeatable outcomes show that cybersecurity is becoming embedded in normal operations.

This maturity-focused narrative helps stakeholders see cybersecurity as an evolving program, not a series of isolated tools.

When and Where to Leverage Metrics

Metrics should be delivered through channels that match their purpose:

- **Annual reports:** Outcomes tied to budget requests and strategic goals.

- **Board presentations:** High-level risk, trends, and maturity indicators.
- **Operational dashboards:** Daily or weekly performance monitoring.
- **Vendor reports:** Supporting evidence for control effectiveness and compliance.

Bringing It All Together

This guidance is designed to be applied in stages. Start small, select a limited set of metrics that support your priorities, and present them consistently using visuals and short narratives.

As you apply this guidance:

- Review metrics regularly and retire those that no longer support decision-making.
- Reuse the same core metrics across audiences, adjusting only the framing and level of detail.
- Focus on trends and outcomes rather than one-time snapshots.

When used intentionally, cybersecurity metrics turn data into insight, insight into strategy, and strategy into action. Over time, they become a shared language that helps leaders, practitioners, and partners understand where the program is today and where it needs to go next.

Understanding Cybersecurity Maturity Models

Over time, trends in metrics can help describe whether a cybersecurity program is ad hoc, developing, defined, managed, or optimized, without requiring deep technical explanations.

- **Ad hoc**: Activities are informal, reactive, and inconsistent.
- **Developing**: Basic processes exist, but they are inconsistently applied or documented.
- **Defined**: Processes and controls are documented, communicated, and generally followed.
- **Managed**: Metrics are used regularly to monitor performance and guide improvements.
- **Optimized**: Continuous improvement is driven by metrics, risk trends, and lessons learned.

Important Caution on Using Maturity Ratings

Maturity models should be applied **intentionally and in context**:

- Target maturity levels should be based on risk and the defined needs of the district, not applied uniformly across all areas.
- A maturity rating or scale is not analogous to a grading scale. Lower maturity in some areas may be appropriate where risk is low or compensating controls exist.
- The purpose of maturity discussions is to support prioritization and investment decisions, not to "score" the cybersecurity program.

Used correctly, maturity models help leaders focus on risk reduction and mission support rather than checkbox compliance.

CoSN is vendor neutral and does not endorse products or services. Any mention of a specific solution is for contextual purposes.