From Metrics to Meaning: Transforming Medical Device Cybersecurity into a Strategic Risk Narrative

TLP:WHITE This report may be shared without restriction.

Contents

List of Tables

Introduction

Medical device manufacturers are generally proficient at generating cybersecurity data. Product security organizations produce data from product Software Bill of Materials (SBOMs), vulnerability management platforms, quality system action, regulatory process actions at scale. Yet many organizations struggle to translate that data into a clear story about risk, security posture, and business impact.

The challenge lies not just in collecting data and metrics, but in creating meaning. Technical teams often track activity and operational performance, while executives need insight into enterprise risk, regulatory exposure, product resilience, and patient safety. Without a common framework, organizations can become data-rich but insight-poor.

Written by and for medical device manufacturers, this paper presents a practical approach for transforming cybersecurity metrics into a structured risk narrative. Its purpose is not to collect more data, but to help organizations identify the metrics that matter, connect operational measurements to executive decision-making, and demonstrate how product security efforts reduce risk, protect patients, and build trust in medical technology.

Ultimately, cybersecurity metrics are most valuable when they do more than measure activity. They should explain how an organization is managing risk, improving resilience, and earning the confidence of regulators, customers, and patients.

The Current State: Data-Rich, Insight-Poor

Medical device manufacturers have entered a new era of cybersecurity accountability—one defined by **regulatory pressure, expanding product complexity, and the critical importance of patient safety**.

Organizations today generate vast amounts of security data across:

- **Vulnerability management systems**
- **SBOM and supply chain analysis**
- **Quality and regulatory systems**
- **Customer and operational environments**

Despite significant investment in tooling and data collection, many organizations still struggle to answer fundamental business questions:

- **Are we reducing real-world risk?**
- **Are our products becoming more secure over time?**
- **Are we aligned with regulatory expectations and market expectations?**

The Failure to Turn Metrics into Meaning

The core problem is not a lack of metrics it is a failure to transform metrics into decision-driving insight.

Fragmentation of Data and Context

Security data is distributed across disconnected systems:

- Vulnerability monitoring tools
  (e.g. SBOM, Dependency-Track, Known Exploited Vulnerabilities (KEV) feeds)
- Issue tracking systems (Jira, quality systems)
- Regulatory and audit systems

The Illusion of Coverage

Organizations often track:

- Total vulnerabilities
- Number of scans
- Number of tests

Yet the data shows there are hundreds of thousands of known vulnerabilities globally and only a small subset are actively exploited in real-world attacks.

This creates a critical issue where treating all vulnerabilities equally dilutes focus and obscures business risk.

Misalignment Between Technical Metrics and Business Decisions

Different audiences require different views:

- Operational teams need granular tracking (e.g., remediation timelines, defect density)
- Executives need strategic indicators (e.g., potential recalls, regulatory findings, financial risk)

However, most organizations mix these levels indiscriminately and fail to translate between them. This results in:

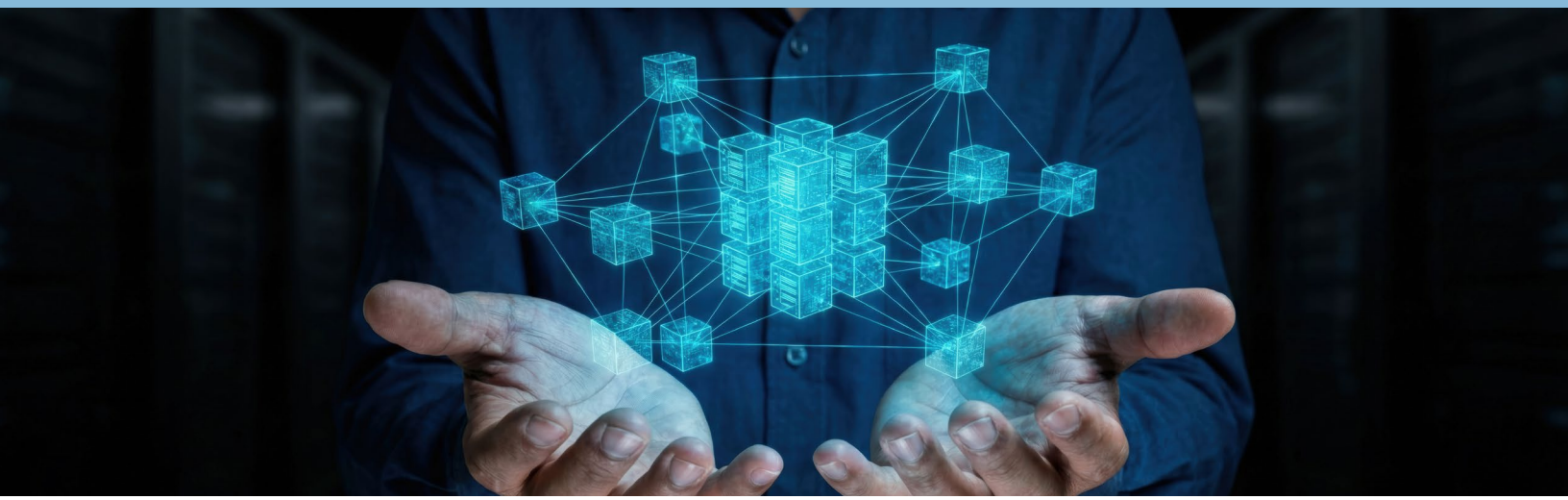
- Technical teams optimizing activity
- Leadership making decisions without clear risk context
- Difficulty in translating security data into business decisions

The Cost of Misalignment

When metrics alignment to business fail, consequences cascade across the business:

- Regulatory submission delays due to deficiencies
- Field corrective actions (recalls, corrections) increasing cost and risk
- Business Risk resulting from unsupported (End of Life (EOL)/ End of Support (EOS)) software (i.e. lack of customer confidence, etc.)
- Loss of market trust and competitive positioning

This creates a critical issue where treating all vulnerabilities equally dilutes focus and obscures business risk.



Building a Structured Measurement Framework

To resolve this perceived disconnect, organizations must evolve from simple data collection to metrics architecture. Below are 4 steps to define the framework.

Step 1: Establish Metric Categories That Align to Risk

The emerging model organizes metrics into four strategic pillars:

A. **Vulnerability Management & Operations** — Measures the organization's ability to identify and resolve security defects:

- Defect density (percentage of vulnerabilities remediated)
- Time from identification to patch readiness
- Time to field deployment (tracked via milestone adoption)

B. **Compliance, Audit, and Risk** — Measures regulatory and quality health:

- Internal audit findings and aging Corrective and Preventative Actions (CAPAs)
- Regulatory submission deficiencies
- External inspection findings (Food and Drug Administrative (FDA) and others)
- Field corrective actions (recalls and corrections)

C. **Lifecycle & Asset Management** — Measures the security of the product portfolio over time:

- Inventory completeness (attack surface visibility)
- Manage and plan for updates due to third-party EOL/EOS software
- Legacy systems with risky, complex vulnerability monitoring

D. **Strategic Maturity & Investment** — Measures long-term program strength:

- Ongoing industry maturity benchmarking (i.e JSP ("Joint Security Plan")
- Security investment relative to Research & Development (R&D) budget
- Workforce capability (trained personnel, security champions)

Step 2: Focus on What Actually Matters — Risk Prioritization

Effective programs prioritize:

- Known Exploited Vulnerabilities (KEV)
- Top exploited vulnerabilities identified by government and industry

These represent:

- A small subset of vulnerabilities
- But the highest probability of real-world exploitation

This shift enables organizations to move from:

Volume-based remediation → Threat-informed prioritization

Step 3: Connect Metrics to Source Systems

A key benefit from the data is explicit mapping:

Metric Type	Source System
Defect Density	SBOM, vulnerability monitoring systems
Patch Timelines	Issue tracking systems
Audit Findings	Quality Management System or equivalent
Regulatory Deficiencies	Regulatory action tracking systems
Product Inventory	Manual or automated asset systems

Table 1: Product Metrics with Sources

This mapping ensures:

- Traceability
- Data integrity
- Repeatability of reporting

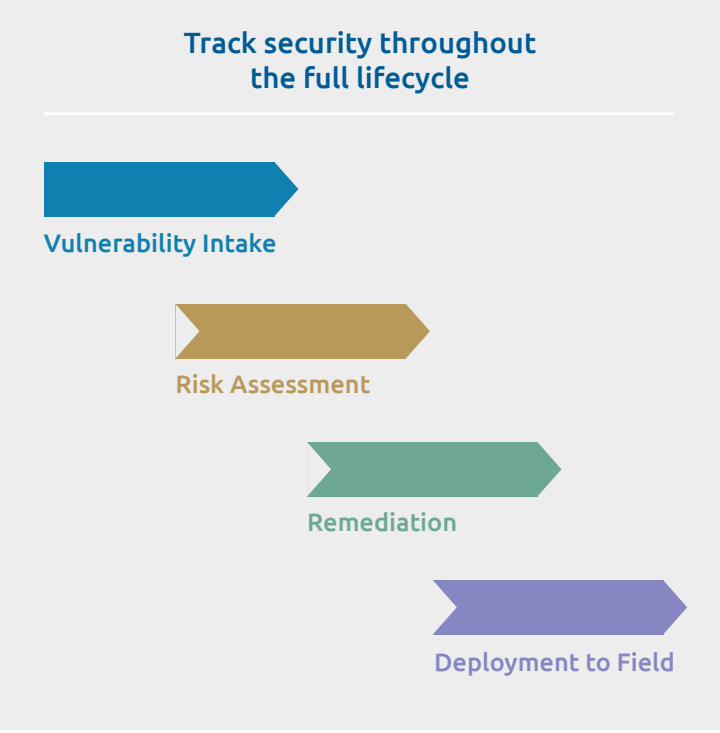
Step 4: Measure the Full Lifecycle

Security must be tracked from:

- Vulnerability intake
- Risk assessment
- Remediation
- Deployment to field

With metrics such as:

- Time to severity determination
- Time to remediation
- Deployment coverage (25%, 50%, 75%, 90%)



The Breakthrough Insight

The transformation hinges on a single insight: Metrics alone do not create value—metrics only matter when they are organized into a narrative of risk that can influence a decision.

From Measurement to Narrative

Leading organizations do not ask:

- "How many vulnerabilities do we have?"

They ask:

- "What risk do these vulnerabilities create?" (i.e. exploitability)
- "How quickly are we reducing that risk?"
- "What is the impact on patient safety and business performance?"

Metrics as a Strategic Language

A mature metric system translates (metrics below include, but are not limited to):

Technical Metric	Business Meaning
Defect Density	Operational maturity and risk exposure
Remediation Time	Responsiveness to emerging threats
EOS/EOL Software	Long-term structural risk
Field Corrective Action (FCA) Events	Direct financial and safety impact
Industry Benchmark	Competitive and industry positioning

Table 2: Technical Metrics and Business Impact

Alignment to Enterprise Risk

All metrics ultimately connect to:

Patient safety • • • Product reliability • • • Regulatory compliance • • • Patient safety

This alignment transforms cybersecurity into a core enterprise risk discipline, not a technical function.

Implementing the Model

Organizations operationalize this transformation by adopting an implementation model that connects daily security execution to enterprise decision-making.

A Dual-Layer Metric Model

In a Dual-Layer Metric Model:

- operational metrics answer whether teams are executing effectively according to their procedures
- executive metrics answer whether the actions of the operational teams are reducing enterprise risk

At the operational level, organizations track defect density, remediation timelines, KEV-focused prioritization, and field deployment milestones. At the executive level, those same signals roll up into business indicators such as inspection readiness, field corrective action risk, lifecycle exposure from unsupported software, competitive maturity, and investment adequacy. This model allows technical data to become a business narrative: not simply how much work was done, but whether that work meaningfully reduced regulatory, financial, and patient-safety risk.

The table on the next page shows how the same underlying security data can be presented at two levels: one for managing execution and one for guiding enterprise decisions.

(*"Typical Source System" data will vary between organizations. These are samples of what was observed across several organizations)

Layer	Metric	What It Measures	Why It Matters	Typical Source System*
Operational	Defect Density	Percentage of identified vulnerabilities that are updated or patched	Indicates security operations maturity and whether vulnerabilities are being corrected effectively	SBOM and vulnerability monitoring systems
Operational	Time from Identification to Patch	Duration from vulnerability discovery to patch readiness	Measures response velocity and exposure window	Issue tracking system
Operational	Time to Severity Determination	Average days from identification to severity and impact determination	Shows how quickly teams understand business relevance of a finding	Vulnerability monitoring plus issue tracking
Operational	Field Deployment Milestones	Progress of field updates at 25%, 50%, 75%, and 90%	Demonstrates whether fixes actually reach deployed devices	Issue tracking and deployment tracking systems
Operational	KEV / Top 15 Older Than XX Days (XX represents an organization's tolerance)	Presence of highly exploited vulnerabilities remaining open beyond XX days	Shifts remediation from volume-based to threat-informed prioritization	SBOM, KEV feeds, and product inventory
Executive	External Inspection Findings	Cybersecurity-related findings from FDA or non-FDA inspections	Leading indicator of further scrutiny and possible corrective action	Regulatory log and quality system
Executive	Product Security FCAs	Recalls or corrections driven by safety/security defects	Direct indicator of financial impact, regulatory pressure, and patient risk	Quality Management System
Executive	Products with EOL/EOS Software	Unsupported third-party software still present in products	Signals structural lifecycle risk, support burden, and future obsolescence cost	Product inventory, SBOM, and lifecycle tracking
Executive	Industry Maturity Score	Benchmark of product security maturity against industry peers	Shows leadership whether the program is competitively mature	Medical Device Innovation Consortium (MDIC) benchmarking survey
Executive	Investment / Training	Security budget allocation and trained staff	Indicates whether the program is being sustainably funded and institutionalized	Finance, training log, and champions log

Table 3: Types of Metrics

Together, these two layers show how disciplined operational measurement becomes executive insight, enabling leaders to judge not only whether work is being completed, but whether risk is actually being reduced.

How to Map Operational Metrics to Executive Metrics

Executive metrics should not be gathered as isolated data points. They should be derived from patterns, thresholds, and recurring signals in the operational layer. For example, if defect density remains high, remediation timelines lengthen, KEV-related items stay open beyond XX days (as defined by the organization based on their tolerance), or field deployment milestones stall, those operational conditions should be translated into executive concerns such as inspection readiness, field corrective action risk, lifecycle exposure, or the need for additional investment.

In simple terms, operational metrics show whether work is progressing, while executive metrics show whether the organization is becoming safer, more compliant, and more resilient.

Operational Input	What to Look For	Executive Output	Business Interpretation
Defect Density + Time from Identification to Patch	Persistent backlog, slow closure rate, or worsening trend over time	External Inspection Findings / Product Security FCAs	Weak remediation performance increases the likelihood of regulatory scrutiny, corrective action, or field impact
KEV / Top 15 Older Than XX Days	High-risk exploitable vulnerabilities remain unresolved beyond policy threshold	External Inspection Findings / Lifecycle Exposure	Failure to address actively exploited vulnerabilities suggests elevated product risk and possible compliance weakness
Field Deployment Milestones	Updates stall at low adoption milestones or progress is inconsistent across the installed base	Product Security FCAs / Commercial Readiness	A patch that does not reach the field does not meaningfully reduce risk and may create customer or regulator concern
Time to Severity Determination + Inventory Completeness	Slow impact assessment or incomplete visibility into affected products	External Inspection Findings / Industry Maturity Score	Delayed understanding of exposure indicates weak governance, weak visibility, or immature product security processes
Products with Third-Party EOL/EOS Software + Legacy Systems Without Automated Monitoring	Growing unsupported footprint, repeated exceptions, or rising manual monitoring burden	Products with EOL/EOS Software / Investment	Signals structural lifecycle risk and may justify modernization, end-of-support planning, or increased security funding
Audit Findings, Aging CAPAs, Awareness, and Champions	Recurring process failures, delayed corrective actions, or weak security capability development	Industry Maturity Score / Investment	Weak execution patterns often point to broader maturity gaps that leadership must address through governance and resourcing

Table 4: Operational Inputs and Executive Outputs Linkage

For example, a product team may find that defect density has remained flat for two quarters, two KEV-related vulnerabilities have stayed open beyond 90 days, and deployment of the latest patch has stalled below 50 percent of the installed base. **Operationally,** this signals a remediation and deployment problem.

Executively, the same pattern should be reported as elevated inspection readiness risk, greater likelihood of future field corrective action, and evidence that current investment or cross-functional execution may be insufficient. The executive report should therefore do more than restate the numbers; it should explain that risk is not being reduced at the pace required by the organization's security and regulatory expectations.

This mapping should be treated as a management method, not a rigid formula. The goal is not to create a one-to-one mathematical conversion for every metric, but to define clear rules for when operational trends, thresholds, or recurring conditions should trigger escalation into executive reporting. In that sense, the executive layer is a disciplined interpretation of operational reality.

A Continuous Data Pipeline

For this model to work consistently, metrics must flow through a continuous data pipeline that is reliable, repeatable, and connected across the product lifecycle.

- Continuously collected
- Mapped to source systems
- Integrated across lifecycle

A Feedback Loop

Once that data pipeline is in place, the organization can turn measurement into action through a disciplined feedback loop.

- Inform decisions
- Shape prioritization
- Guide investment
- Improve future outcomes

Together, the dual-layer model, the continuous data pipeline, and the feedback loop create the practical operating system that turns cybersecurity metrics from static reporting into sustained organizational learning and risk reduction.

The Future State: A Narrative-Driven Security Program

The end state is not more metrics—it is better understanding.

A Unified View of Risk

Organizations achieve:

- A single, structured view of product security
- Traceable and defensible data
- Alignment across all product lines

A Shift from Reactive to Predictive

With leading indicators and prioritized risk:

- Threats are anticipated
- Resources are focused
- Security becomes proactive

A Stronger Link Between Security and Business Outcomes

Security decisions are now directly tied to:

- Revenue protection
- Regulatory success
- Product competitiveness
- Patient safety

Call to Action

To realize this transformation, medical device manufacturers must:

- Architect a small, structured set of meaningful Key Performance Indicators (KPIs)
- Integrate data across SBOM, vulnerability, quality, and regulatory systems
- Prioritize real-world exploitable vulnerabilities (KEV and Top threats)
- Align metrics across operational and executive audiences
- Communicate metrics as a clear business narrative—not just data

Final Thought

Cybersecurity metrics are not just measurements of activity—they are the mechanism by which an organization explains how it protects patients, manages risk, and earns trust.

Organizations that master this narrative will move beyond compliance—and define the future of secure, resilient, and trusted medical technology.

Special Thanks to the following contributors:

Nancy Brainerd (Medtronic)
Trevor Steen (Abbott)
Chris Gates (arsMedSecurity)
Tomislav Mustac (Mount Sinai)
John Chenowith (Elekta)
Julien Tomassone (Fresenius)
Victoria Averbukh (Stryker)
Esther Adegboye (Stryker)
Dan Lyon (Boston Scientific)
Phil Englert (Health ISAC)
Robert Smigielski (B.Braun)
Luisa Soares de Brito (BD)
Taylor Porter (Health ISAC)
Loshan Wickramasekara (ICON PLC)
Carsten Buettner (Fresenius)
Svetlana Griffin (Baxter)
John Volock (Medtronic)
Citlalli Payan (Amgen)
Stacie Brough (Baxter)
Jason Shutt (Baxter)

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org.