CYBELLUM

2024 Medical Device Security Survey Report

October 2024

Table of Contents

Introduction & Executive Summary

Introduction

The medical device industry has entered a new era of cybersecurity marked by the emergence of expanded regulatory guidelines. At the forefront is the FDA's new cybersecurity guidance, issued in 2023, which provides manufacturers with comprehensive security guidelines for managing product security across the device lifecycle—from design to post-production. This year's report aims to explore how these new guidelines, along with global standards such as those from the EU and the IMDRF, are reshaping priorities and strategies for medical device manufacturers (MDMs).

With a clearer regulatory environment, MDMs now have the need to adopt a more holistic approach to cybersecurity. Our 2024 survey delves into whether this shift has resulted in new challenges, altered priorities, or significant changes in practices. We examine the evolving landscape, focusing on key areas like software supply chain security, post-market compliance, and the methods MDMs use to safeguard their devices.

The findings presented in this report offer a global perspective, capturing trends and insights from product security teams, compliance officers, and other key decision-makers. As the medical device sector continues to adapt to the new regulations, understanding these shifts will be critical in ensuring robust security and compliance across the board.

Methodology

This year's survey was conducted in September 2024 and gathered insights from 250 professionals in the medical device manufacturing sector. The survey focused on individuals with titles in Product Security or Cybersecurity Compliance from companies with 500 or more employees. Respondents were located across key markets, including the US, Germany, and other regions such as the UK, Belgium, Switzerland, Japan, and China.

To ensure relevance, participants were selected from OEMs or suppliers, specifically those involved in medical devices incorporating software, firmware, and connectivity. Their roles spanned Product & Device Security and GRC (Governance, Risk & Compliance), providing a comprehensive view of the industry's current cybersecurity landscape.

Executive Summary

1

The Shift in Priorities: Time-to-Market Takes Precedence Over Device Security

While 95.6% of respondents agree that device security is critical to minimizing business risk and protecting intellectual property, 92.8% now believe that getting products to market is a higher priority than security, up dramatically from 14% in 2023. This shift is more pronounced outside the US and in larger, more mature companies, raising concerns about the potential for long-term security compromises.

2

The Balancing Act: MDMs Face Security-Efficiency Dilemma

Asset management ranks as the top challenge (36.3%), followed by frictionless security with R&D (30.3%) and efficiency (28.3%). These findings highlight the complexity of balancing product security with time-to-market and productivity goals. As MDMs strive to improve compliance, security analysis accuracy, and shifting-left security, these priorities reflect the industry's efforts to enhance both security and operational efficiency.

3

Product Security Maturity Disparities: Regional and Organizational Differences

US companies generally report higher maturity in product security compared to their German and the Rest of the World (ROW) counterparts, with OEMs showing more maturity than suppliers. Smaller companies also tend to demonstrate higher maturity in areas like VEX adoption. However, 54.6% of respondents still rank their software assurance practices at a basic level, and 78% of organizations lack a dedicated product security function, underscoring the overall immaturity of product security programs.

4

Rising Budgets: Driving Security Advancement

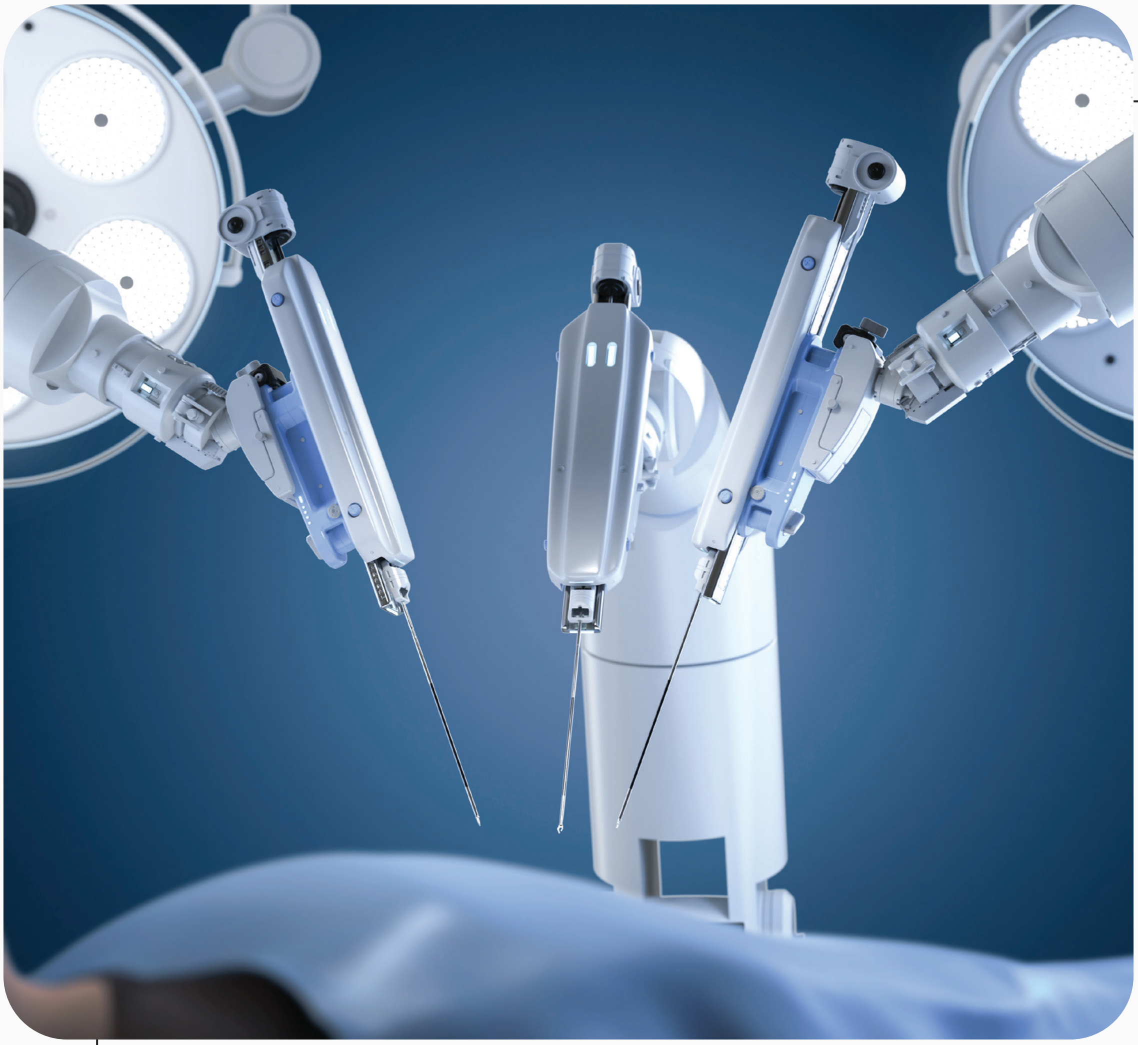
70.5% of respondents reported increasing their security budgets in 2024, up from 49% in 2023. However, the average budget increase was 10.8%, down from 17% the previous year. More mature companies in software assurance are more likely to increase their budgets, reflecting their recognition of the importance of robust security practices.

5

Roles & Responsibilities: Significant Regional Differences

The responsibility for product security is increasingly spread across multiple roles, reflecting a shift in how organizations manage this critical function. While the CPSO or VP Product Security still leads (22.3%, down from 28% in 2023), the CISO (21.5%) and CIO (17.1%) are gaining influence. In Germany and ROW, CISOs take the lead, while the CPSO remains more dominant in the US. However, with 78% of organizations lacking a dedicated product security function, responsibility is often distributed, potentially weakening cohesive security strategies.

Survey Findings



Company's Attitude Towards Device Security

Medical device manufacturers continue to emphasize device security in 2024, with 96% agreeing it is critical for protecting intellectual property and minimizing business risk, up from 91% and 92% in 2023, respectively. Protecting brand reputation is also a priority, with 94% agreeing, slightly higher than last year's 91%.

However, a significant shift has emerged: **93% of respondents now agree that getting products to market is a higher priority than device security, a dramatic increase from just 14% in 2023.**

The tension between speed-to-market and security is more pronounced in non-US regions, as well as in larger and more mature companies.

This shift highlights the growing challenge for manufacturers to balance quick market entry with maintaining robust device security.

The trend suggests a need for further investigation and education to ensure long-term security is not compromised in the race to bring new products to market.

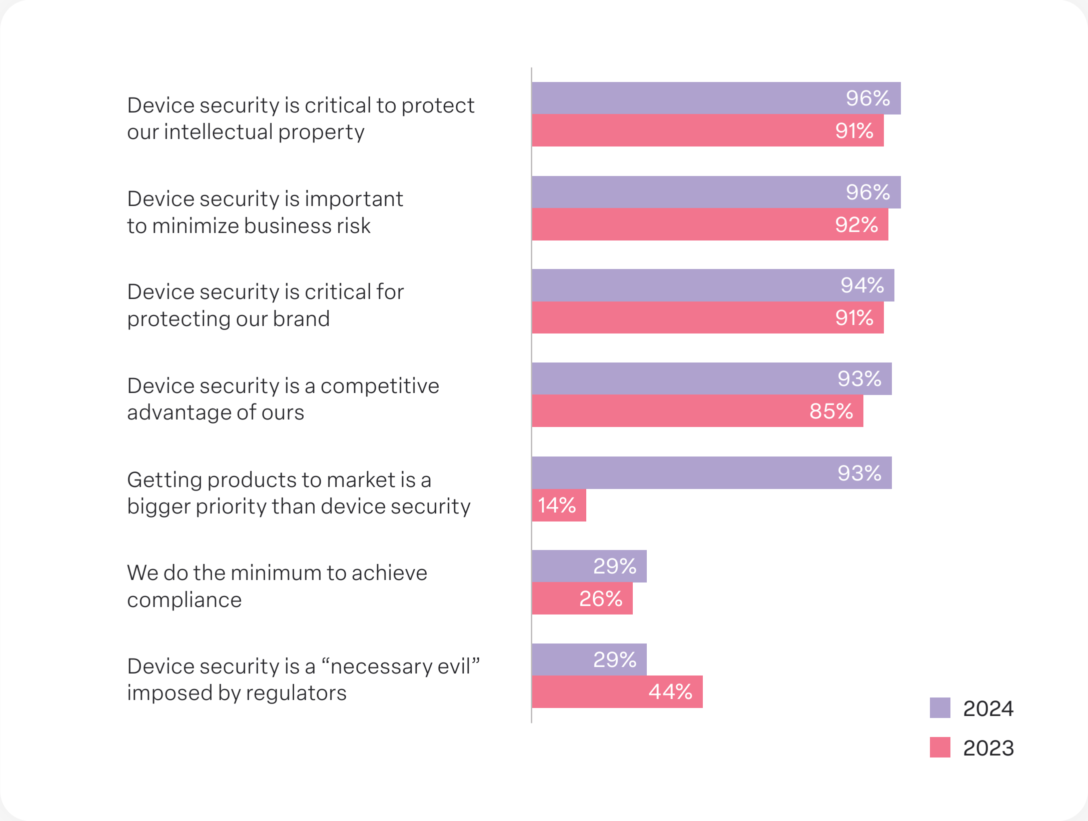


Figure 1: Company's Attitude Towards Device Security

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Maturity Level – SBOM & Asset Management

Most companies (63%) rate their asset management maturity at Level 2, indicating moderate progress beyond the basics. However, there is still room for improvement when it comes to advancing towards higher levels of maturity, which involve greater automation and more precise asset definitions, such as through robust SBOMs.

An important trend is the link between asset management maturity and security assurance maturity.

Companies with lower asset management maturity tend to have lower maturity in areas like vulnerability management and product security assurance. This correlation highlights how foundational asset management practices are essential for effective security.

Without well-defined asset management processes, it becomes challenging to develop advanced security assurance capabilities, underscoring the importance of strengthening asset management to support broader security efforts.

OEMs generally demonstrate higher maturity in asset management compared to suppliers, further underscoring the need for industry-wide improvement.

The current concentration at level 2 suggests that while the industry has moved beyond basic practices, significant growth is still needed to reach more advanced levels.

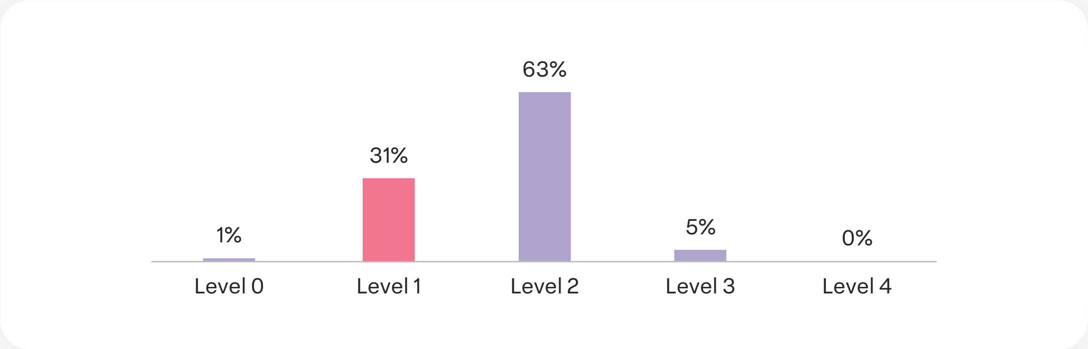


Figure 2: Security Program Maturity – SBOM & Asset Management

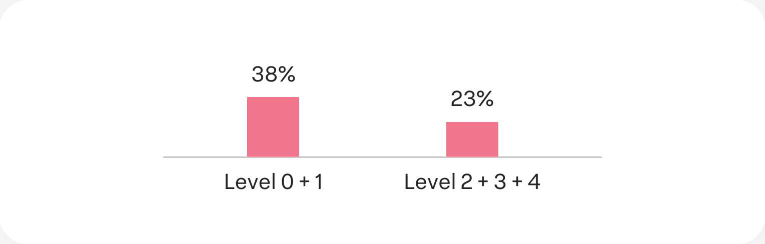


Figure 3: Level 1, by Maturity Level of Security Assurance

Level 0 - We have no asset/SBOM management processes in place

Level 1 - We generate basic SBOMs from one source (binary or source code)

Level 2 - We create and manage high-quality, complete SBOMs by merging data from multiple sources

Level 3 - We have semi-automated SBOM management process, where we create, fix, deduplicate, validate and approve SBOM

Level 4 - we have fully automated asset management and data sharing: we import data automatically from design, to build, to post-production update systems, etc., and have an SBOM sharing portal for customers and/or suppliers

Maturity Level - Security Assurance

Most companies rate their security assurance maturity at fairly low levels. Over half of the respondents (54.6%) are at level 1, while 40% place themselves at level 2. This indicates that many companies are still in the early stages of developing robust security assurance practices, such as around vulnerability management and coding weakness detection.

Suppliers tend to have lower maturity than OEMs, with 64.7% of suppliers at level 1, compared to 47.7% of OEMs.

Again, we see a correlation between security assurance maturity and asset management and compliance maturity, suggesting that advancing in one area can help improve others.

This data reveals that **the industry overall has significant room for improvement to reach advanced levels of maturity, which involve greater automation, integration of multiple security data sources, and optimized workflows** for software security assurance.

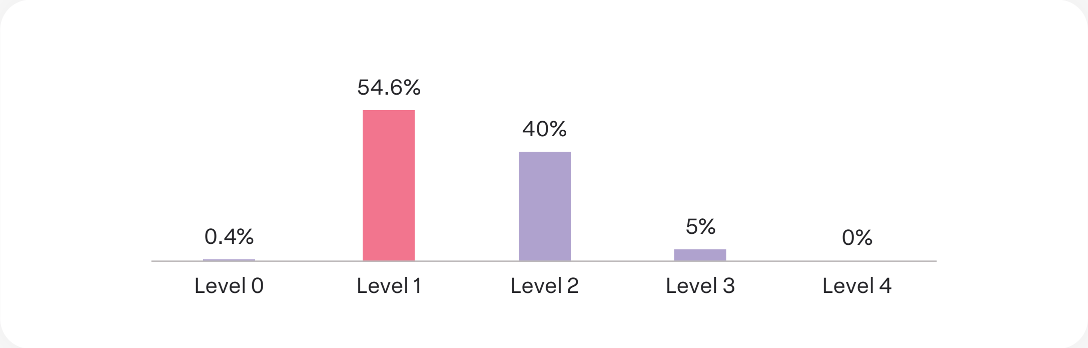


Figure 4: Security Program Maturity - Security Assurance

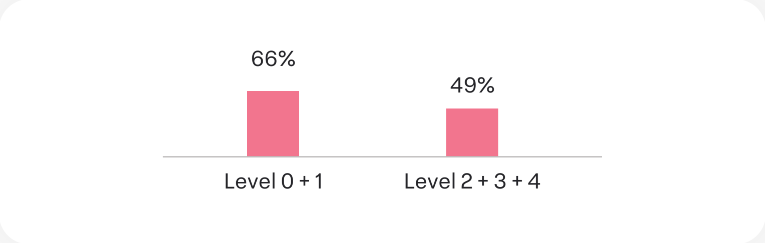


Figure 5: Level 1, by Maturity Level of Asset Management

Level 0 - We have no vulnerability management or other cyber-assurance processes in place

Level 1 - We conduct basic vulnerability monitoring: mapping CVEs to SBOMs relying primarily on the NIST NVD. Lots of manual work.

Level 2 - We do automated smart filtering of CVEs based on product context and impact, exploitability analysis, and matching external feeds with SBOMs

Level 3 - We have a risk data system aggregating vulnerability assessments, threat models, pen tests and fuzzing, enabling comprehensive assurance

Level 4 - We automate the entire assurance process, by connecting the risk data system to both asset data and threat feeds, so risks are detected, triaged, and monitored automatically for all products pre and post production

Maturity Level - Cyber Compliance

Most companies rate their cyber compliance maturity as fairly advanced, with a near-even split between level 2 (49%) and level 3 (50%).

In Germany, 58% of companies place themselves at level 2, while 56.9% of companies in the rest of the world rank at level 3. The US falls in between, with 51.8% at level 2 and 45.9% at level 3.

Notably, very few respondents rated their organizations at levels 0 or 1.
We see a positive correlation between cyber compliance maturity and other competencies like asset management and security assurance. Companies with higher maturity in these areas tend to be more advanced in their cyber compliance efforts as well.

However, this higher level of maturity doesn't always result in higher compliance rates for all regulations and standards. Medical device manufacturers often take a selective approach to compliance, focusing on specific requirements, as explored later in this report.

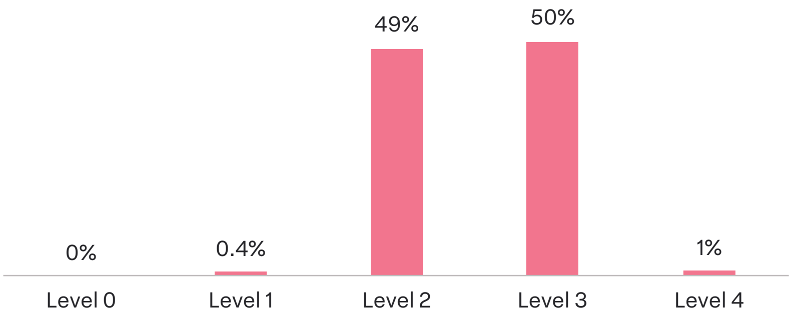
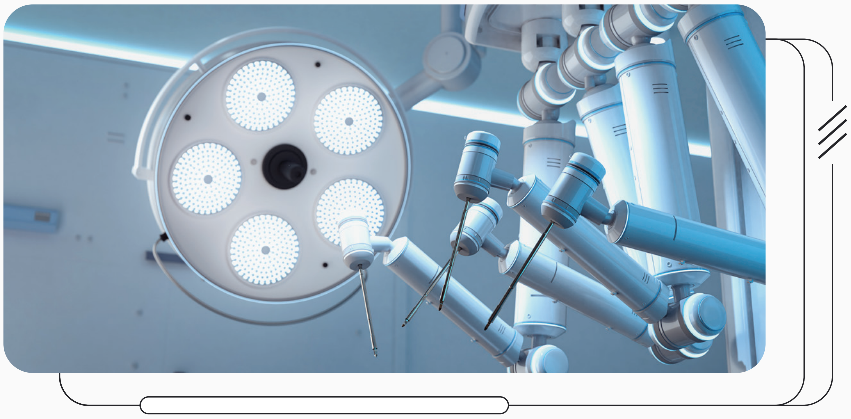


Figure 6: Security Program Maturity - Cyber Compliance



Level 0 - we are not compliant with regulations

Level 1 - We're likely to be caught off guard by an audit since we manually collect compliance data.

Level 2 - We're partially audit-ready with a centralized repository for some compliance evidence, like SBOMs, but not everything is covered.

Level 3 - We're audit-ready with automated evidence management: reports are auto-generated from existing system data, like SBOMs and security assurance activities.

Level 4 - We're ready even before the auditor comes - we have full integration of evidence data into QMS, PLM/ALM, and other systems. Compliance is seamlessly integrated into the development lifecycle.

Maturity Level - Risk Management and Governance

Most companies rate their risk management and governance maturity at a fairly advanced level, with 51% at level 2 and 47% at level 3.

In Germany, the maturity level is particularly high, with 68% of respondents placing themselves at level 3. In contrast, companies in the US and the rest of the world primarily rank themselves at level 2 (58.8% and 54.3%, respectively).

Notably, no respondents ranked their organizations at levels 0 or 4, and only 2% ranked them at level 1.

Interestingly, suppliers tend to rate themselves more mature in risk management, with 57.8% at level 3, compared to 38.9% of OEMs. Most OEMs remain at levels 1 and 2 (61.1%).

While maturity in this area is generally high, it does not show a positive correlation with other product security aspects. In fact, 61.8% of companies at level 3 in risk management are still at levels 1 or 2 in compliance, suggesting a gap in holistic security advancement.

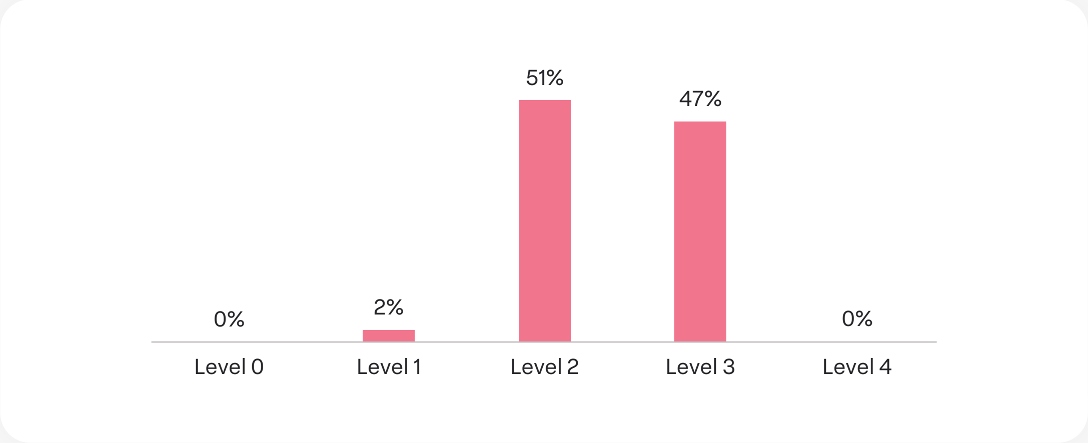


Figure 7: Security Program Maturity - Risk Management and Governance

Level 0 - We do not have such a thing in our organization

Level 1 - Risk status has to be pieced together manually based on data from multiple sources.

Level 2 - Partial risk management: dashboards exist for some risk management areas, such as lists of vulnerabilities in products, data is updated infrequently, no defined playbooks (such as in SOAR), or real time alerts.

Level 3 - Risk management automation: Dashboards are automatically updated thanks to some integrations with asset data and/or vulnerability/risk data. Real-time alerts are set up for critical issues. Playbooks exist. Additional data sources are managed and tracked in a centralized location.

Level 4 - Fully Integrated Risk Management: Full integration into enterprise systems as well as asset management, risk data, and compliance data to provide a 360-degree picture of risk for every product at any given time. All relevant asset sources (CI/CD, SBOMs) and finding sources (TARA, Threat feeds, PSIRT feeds, Pen testing results, etc.) are integrated into a centralized system. Full response automation - response is quick with both real-time alerts and playbooks.

Confidence in Timely Response to Post-Market Security Incidents

A significant 76% of respondents expressed confidence in their ability to address post-market cyber risks in medical devices promptly. This marks an increase from 70% in 2023, reflecting growing confidence in managing security incidents.

Notably, Germany had the lowest confidence levels, with 32% of respondents reporting they were “not very confident,” compared to 24.1% in the rest of the world (ROW) and 18.8% in the US.

There is a clear correlation between product security maturity levels and confidence in addressing post-market incidents. Companies with lower asset management and compliance maturity (levels 0 and 1) reported less confidence in their incident response abilities. Conversely, more mature companies in software assurance (levels 2 and 3) were significantly more confident, with 23% being "very confident," compared to just 7% at lower maturity levels.

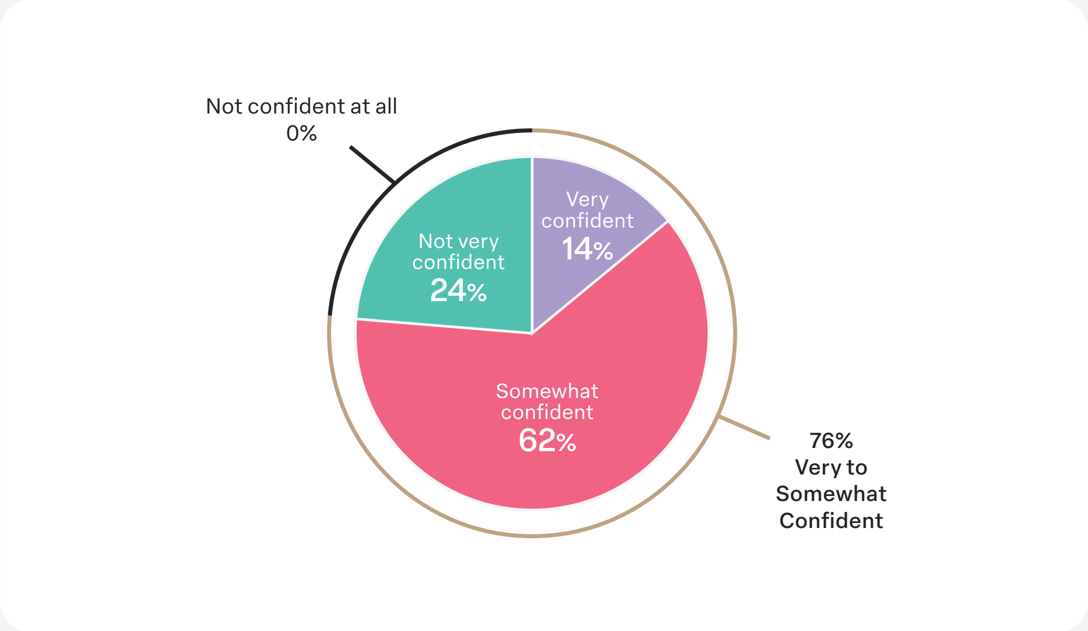


Figure 8: Confidence in Mitigating Post-Market Device Cyber Risks in a Timely Manner

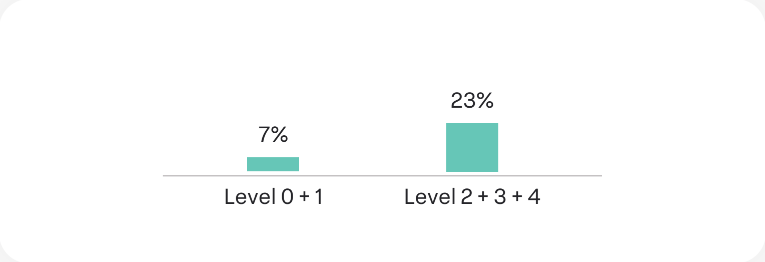


Figure 9: Very Confident, by Maturity level of Security Assurance

Organizational Ownership for Medical Device Security

In 2024, ownership of product security has shifted from a somewhat centralized model in 2023 to a more dispersed, multi-stakeholder approach.

The Chief Product Security Officer (CPSO) or VP of Product Security remains the top role, but its dominance has decreased to 22%, down from 28% last year. Meanwhile, the CISO now manages security for 22% of organizations, a 4.5% increase.

Notably, the Chief Information Officer (CIO) has risen from sixth place to third, now overseeing product security in 17% of companies.

This shift reflects how companies are aligning ownership with the product security process itself, which involves multiple activities—ranging from security and development to compliance and management. The trend is also visible regionally: In the US, the CPSO still leads, while in Germany and the rest of the world, the CISO and CIO have gained prominence.

Interestingly, the CIO's growing role contrasts with the declining influence of compliance and quality functions. The CPSO is still more common among OEMs and smaller companies, while compliance and GRC roles dominate in more mature organizations. Despite these shifts, **78% of companies still lack a dedicated product security function, highlighting the immaturity that persists in many programs.**

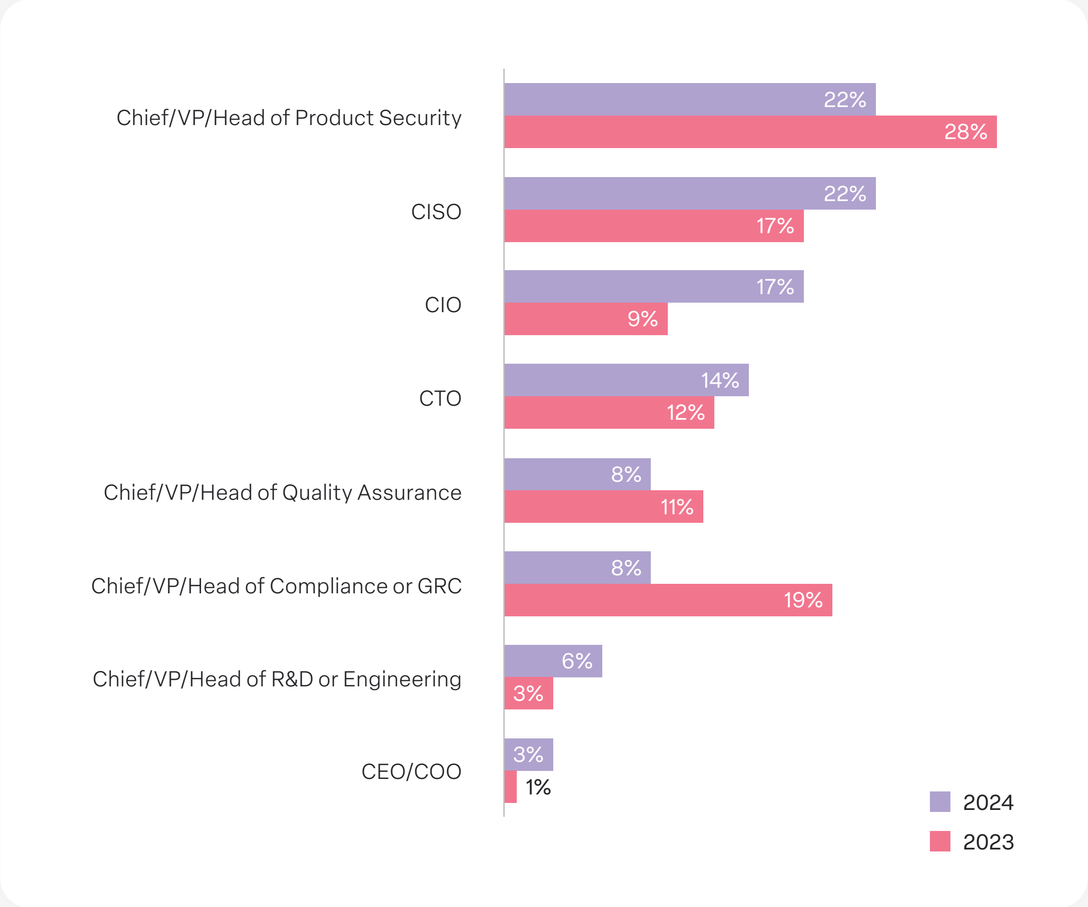


Figure 10: Organizational Ownership for Medical Device Security

Top Medical Device Security Challenges

The main device security challenges in 2024 are asset management (36%), frictionless R&D processes (30%), and efficiency (28%). Asset management's prominence reflects rising regulatory focus, while **efficiency's leap from 5th place last year, alongside the need for smoother R&D processes, indicates growing recognition of security's impact on time-to-market and productivity.** Companies at lower maturity levels particularly struggle with efficiency compared to mature ones (fig. 12).

Two notable shifts this year include a drop in concern over managing multiple tools, from 3rd in 2023 to 9th in 2024 (22%), and a decline in headcount growth, from 4th to 11th.

These shifts suggest that economic pressures, such as competition and inflation, prompt MDMs to prioritize technology optimization and operational efficiency over expanding cybersecurity teams.

Breaking down the data reveals further complexities:

- Asset management is a top challenge in Germany (48%) but less in the US (31.8%), and is more of a challenge for suppliers (44.1%) than OEMs (30.9%).
- Frictionless security with R&D ranks #2 in the US, but is a lesser concern elsewhere.
- Efficiency ranks #1 in Germany (42%) and ROW (30%), but much lower in the US (17.6%).
- Continuous product security management is the top challenge in the US (41.2%), but ranks 5th in Germany and 11th in ROW.
- Software supply chain security is a significant challenge in Germany (38%, ranked 3rd) but ranks near the bottom elsewhere.

These challenges illustrate the complexity of medical device security, as manufacturers navigate multiple concerns of similar weight, spanning regional and organizational differences.

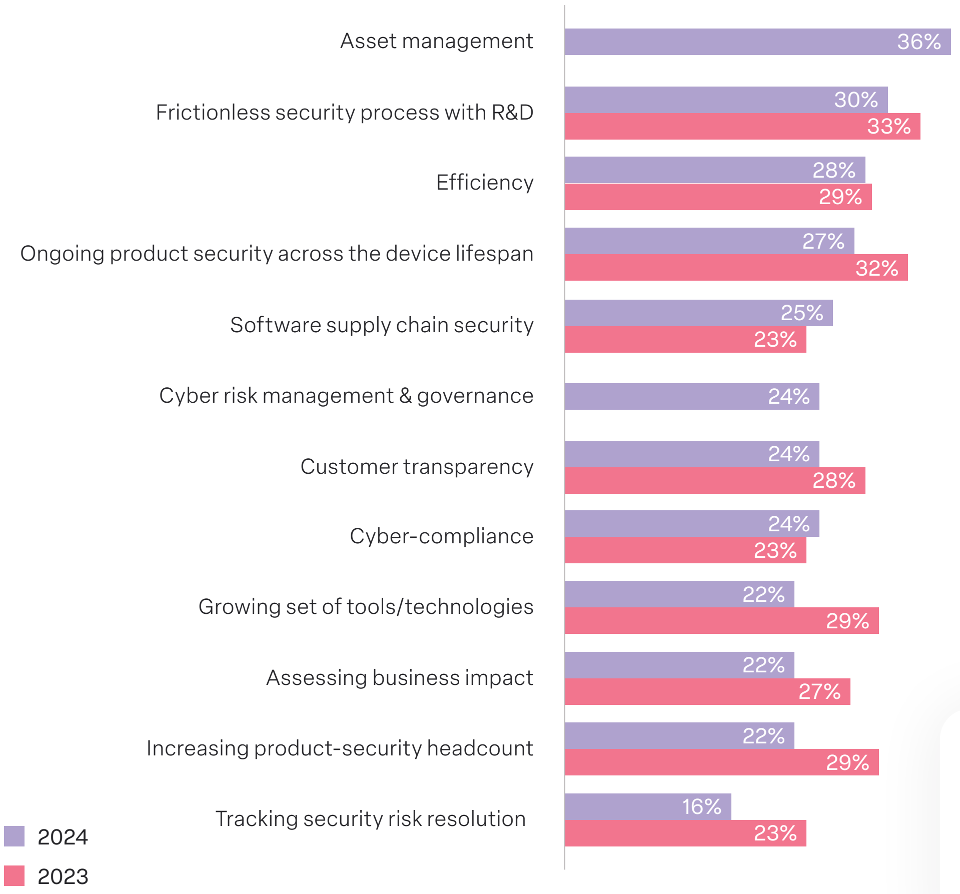


Figure 11: Top Device Security Challenges

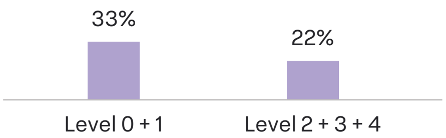


Figure 12: "Efficiency", by Maturity level of Security Assurance

Top Priorities for Product Security Roadmap

The top priority for MDMs in 2024 is improving compliance submission success (32%), followed closely by enhancing security analysis accuracy (31%), which rose from 8th place last year. This is particularly important for mature companies (fig. 14). Shifting-left security holds third place (31%).

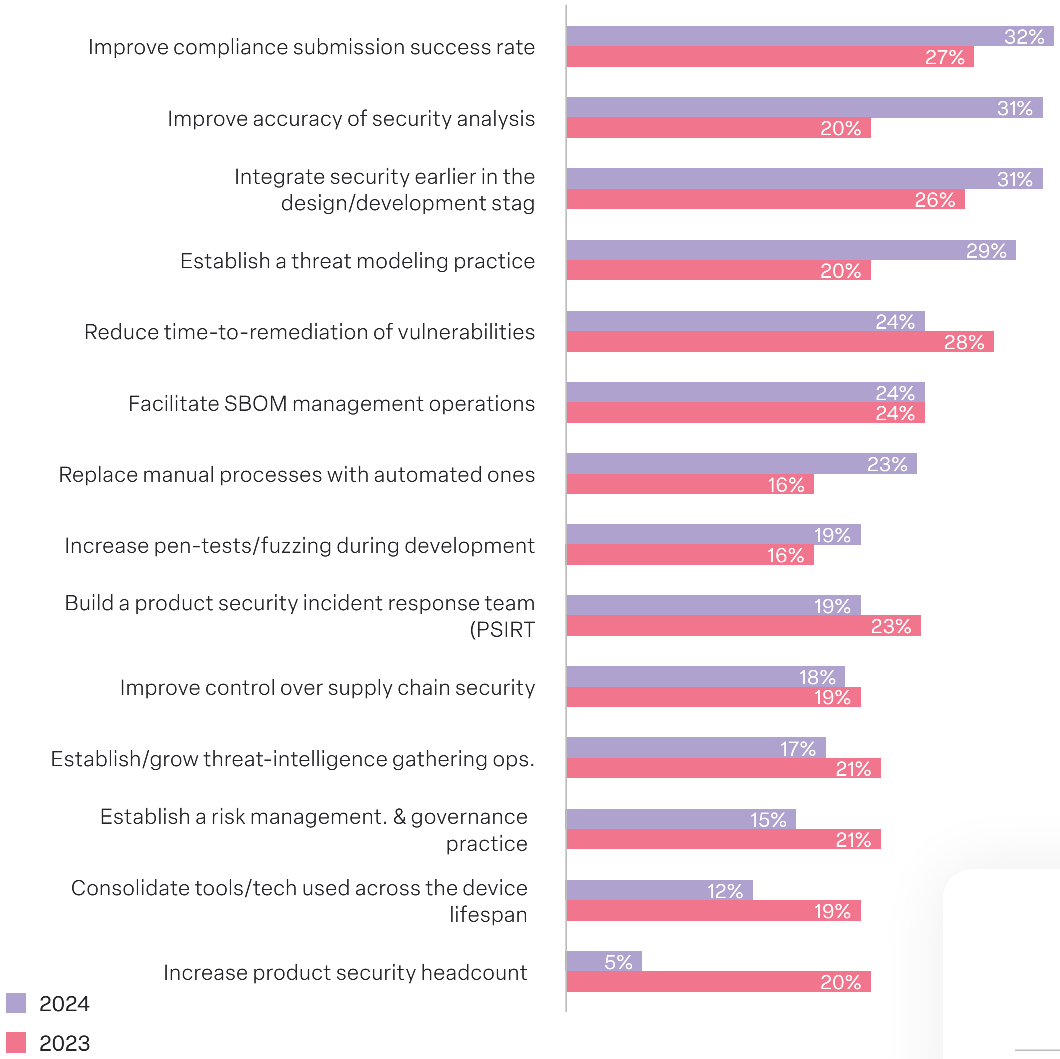
Notably, reducing vulnerability remediation time, the top priority in 2023, dropped to 5th place (24%).

A deeper look reveals regional differences - **In the US, building a PSIRT and automation are top priorities, while in other regions, threat modeling is key.** Compliance, while a top concern globally, ranks lower outside of the US, most likely because the strongest compliance regulations come from the FDA.

OEMs place greater emphasis on reducing time to remediation and threat modeling, while more mature companies in risk management prioritize security analysis accuracy and threat modeling over compliance.

Automation also ranks higher this year, likely driven by the focus on efficiency as a top challenge.

Industry commitment to threat modeling (29%), SBOM management (24%), and incident response (23%) remains strong, aligning with regulatory best practices.



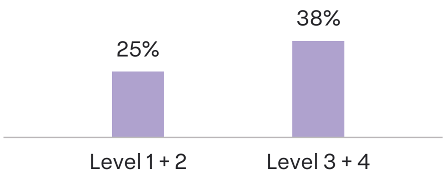


Figure 13: Top Priorities for Product Security Roadmap

Figure 14: “Improve accuracy of security analysis”, by Maturity level of Risk Management & Governance

Complying With Cybersecurity Regulations, Standards, and Guide

The top regulations and standards that medical device manufacturers comply with are the FDA's Content for Premarket Submissions (71%), the EU MDR/IVDR (66%), and the Omnibus bill's cybersecurity requirements (62%).

However, regional disparities reveal different compliance priorities:

- In the US, 98.8% of companies comply with both the FDA's premarket and postmarket requirements, while 90.6% follow the Omnibus requirements. Beyond these, other standards, such as IEC 81001-5-1, see much lower compliance (26%).
- In Germany, 96% of companies prioritize the EU MDR/IVDR, followed by 60% for the FDA's premarket requirements and 56% for IEC 81001-5-1. Compliance with other standards ranges from 20% to 50%.
- Elsewhere, compliance is led by the EU MDR/IVDR (83%), followed by IEC 81001-5-1 (56.9%) and the Omnibus requirements (46.6%).

This year has seen a shift in compliance priorities, with the FDA's premarket guidance rising from 4th to 1st place, while IMDRF dropped from 1st to 6th.

Despite regional differences, MDMs remain committed to improving compliance, aiming for over 90% adherence to most regulations within the next year.

Inconsistent global compliance patterns suggest a need for more harmonized international standards, a sentiment echoed by many manufacturers.

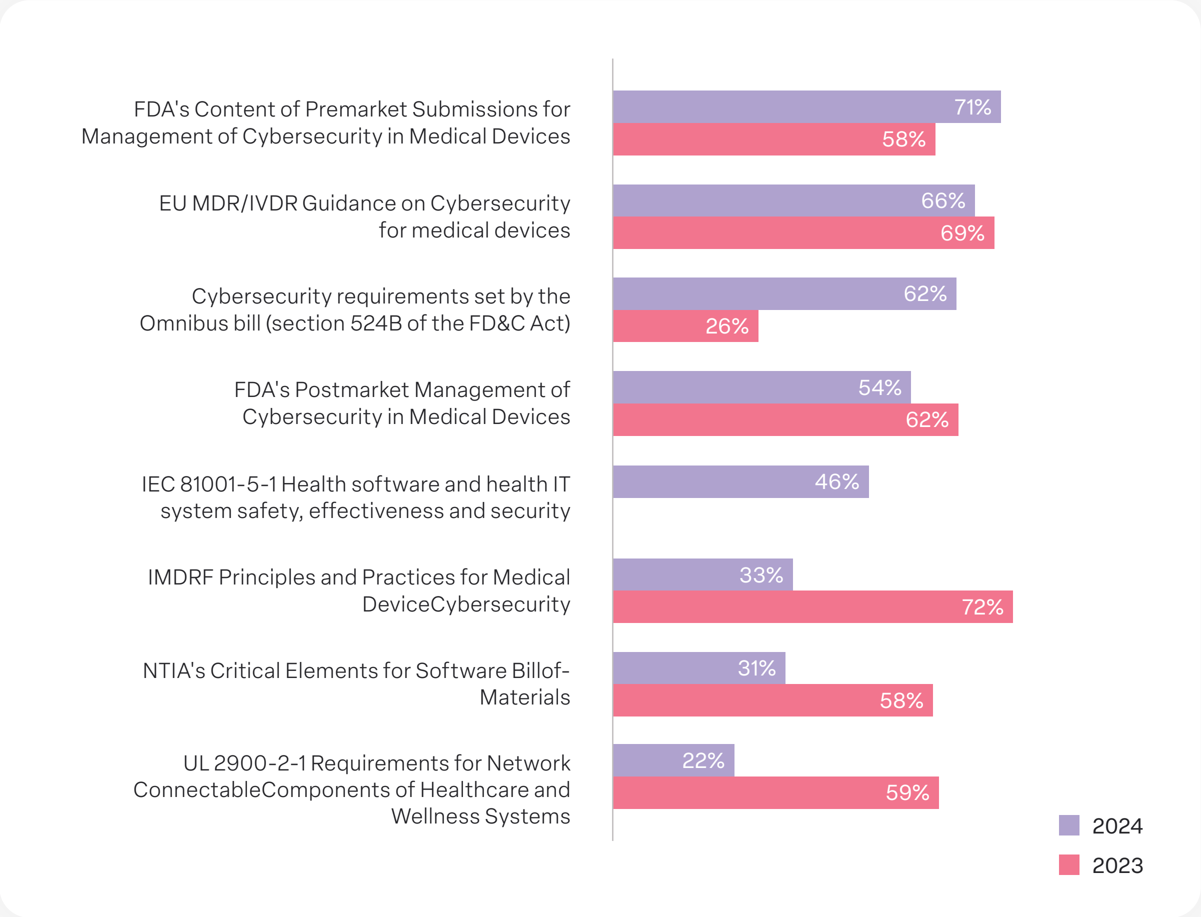


Figure 15: Compliance with Medical-Device Security Regulations & Standards

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Product Security Budget Changes

In 2024, **70% of medical device manufacturers reported an increase in their device security budgets, a significant jump from 49% last year.** Meanwhile, 20% of companies kept their budgets unchanged, and 10% reported a decrease, compared to just 1% in 2023. However, the average budget increase was smaller this year, at 10.8%, down from 17% last year.

Two key insights emerge from the data:

- In the US and ROW, 76% and 73% of companies, respectively, increased their budgets by up to 25%, while in Germany, budgets mostly remained unchanged (~30%) or even declined (16%).
- More mature companies in software assurance saw higher budget increases, while less mature companies reported budget decreases of up to 10%.

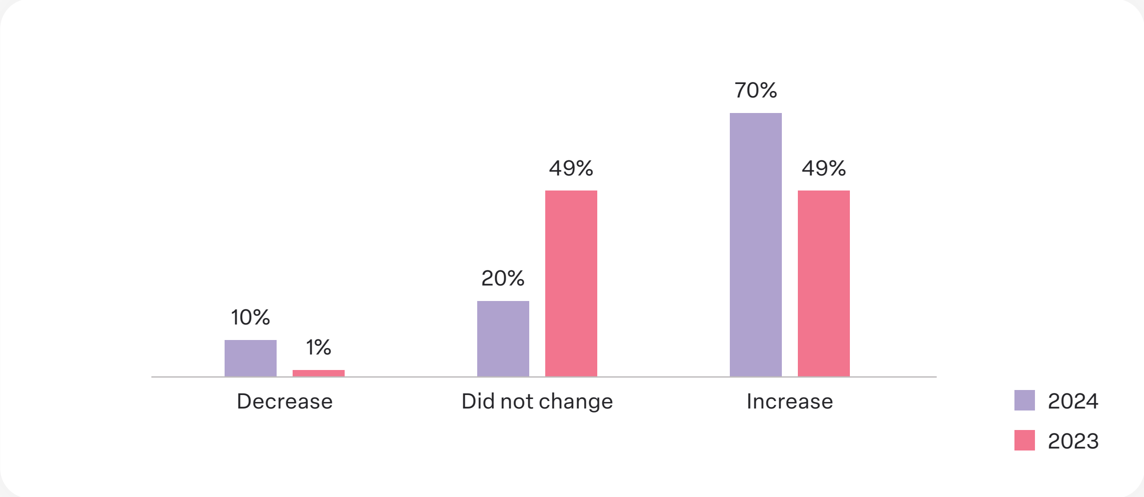


Figure 16: Product/Device Security Budget, 2024 vs. 2023

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Common Practices Used to Address Software Supply Chain Security Risks

Medical device manufacturers have adopted several key practices to secure their supply chains. A significant 86% of respondents now request SBOMs from suppliers to support their own efforts, up from 61% in 2023, with more mature companies in cyber compliance adopting this practice than less mature ones.

Additionally, 86% of companies maintain up-to-date SBOM databases, a rise from 77% last year. This practice Vis especially common among companies with higher asset management and cyber compliance maturity levels.

While 85% of respondents track supplier security KPIs, this figure has slightly decreased from 87% in 2023, with advanced risk management companies (level 3) more likely to track KPIs than less mature companies (levels 1+2).

Generation of VEX advisories remains low at 13%, but over 80% plan to implement this practice in the next 12 months, particularly among mature asset management companies. Currently, 24% request VEX advisories from suppliers, with adoption significantly lower in Germany compared to the US and ROW.

The overall trend shows that **more mature companies are adopting a broader range of practices to enhance supply chain security.**

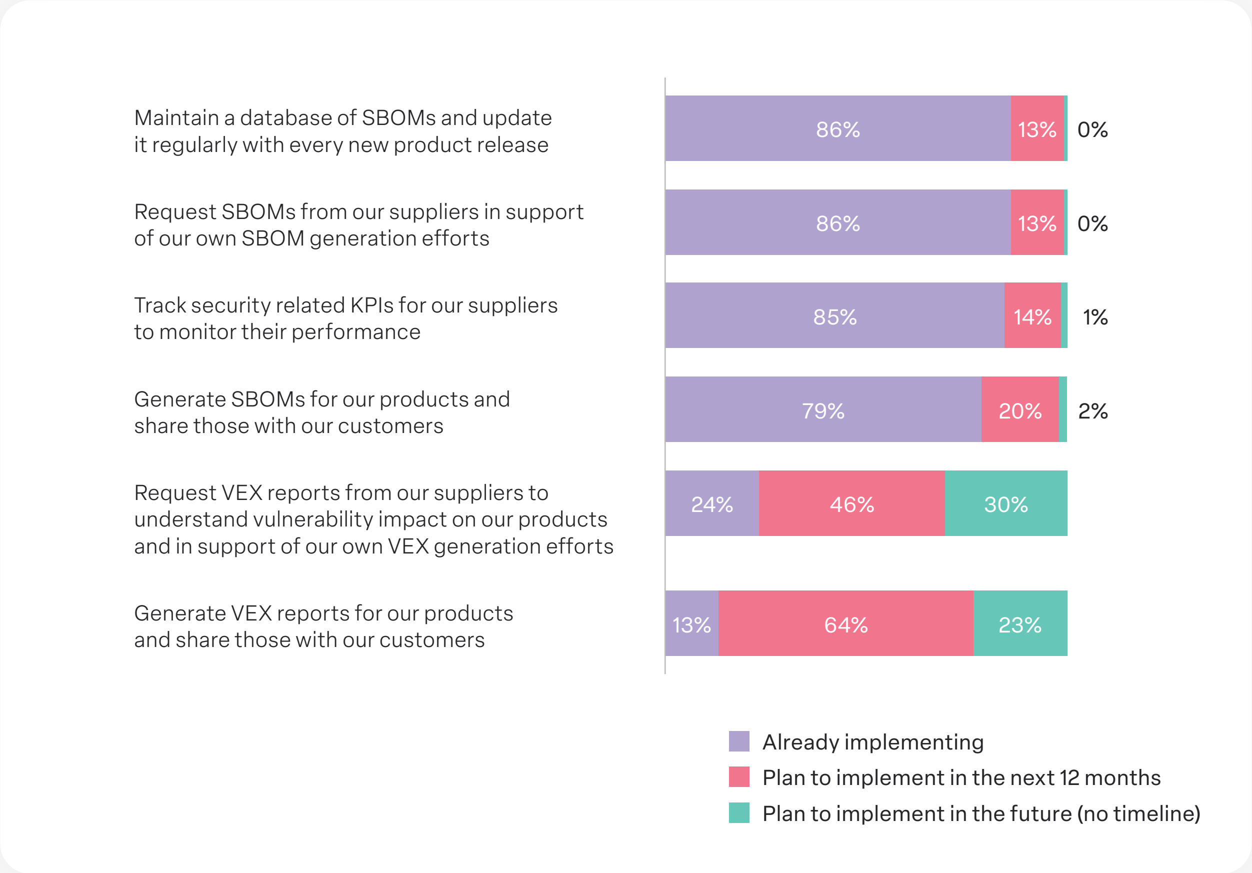


Figure 17: Common Practices Used to Address Software Supply Chain Security Risks

Product Security Practices Requiring Improvement

In 2024, **incident response remains the top product security practice needing improvement (39%), followed by threat modeling (33%),** which rose from third in 2023. Risk management and governance climbed to third (32%) from fourth in 2023.

Other key areas include cyber compliance readiness, which dropped from 2nd to 4th, and threat intelligence gathering, which rose to 5th place.

Threat modeling is a more prominent issue in Germany compared to the US and ROW. In contrast, overall risk management and governance is the top issue in the US and for OEMs. CVE management is a bigger concern in the US and for companies with immature risk management.

Interestingly, SBOM management has dropped from 5th to 8th, likely because most companies consider themselves relatively mature in asset management.

These findings align with regulatory priorities, emphasizing the need for medical device manufacturers to address complex product security and compliance efforts to achieve their goals.

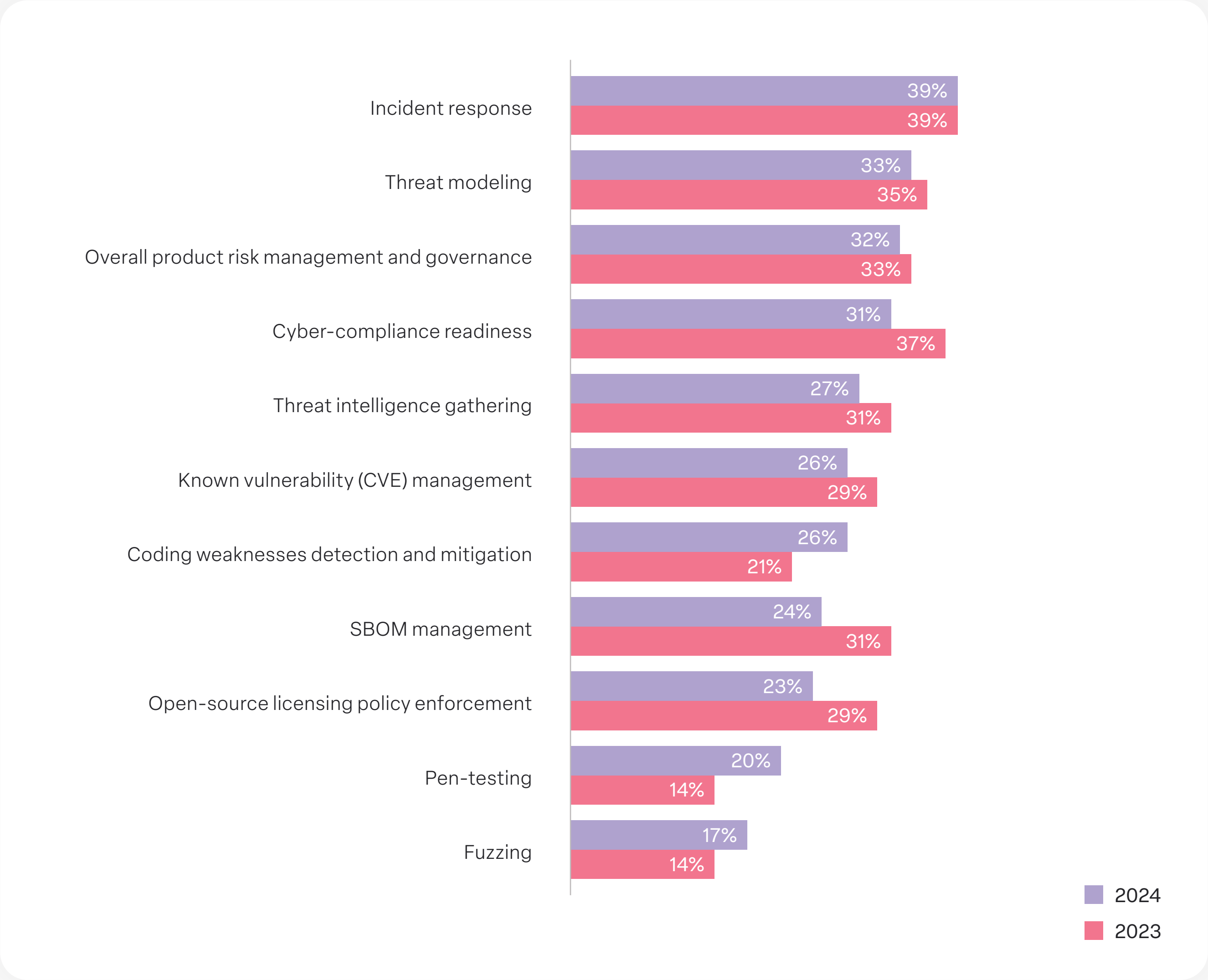


Figure 18: Product Security Practices Requiring Improvement

Demographics

Country, Companies Characteristics, Job Seniority, Areas of Work, and More

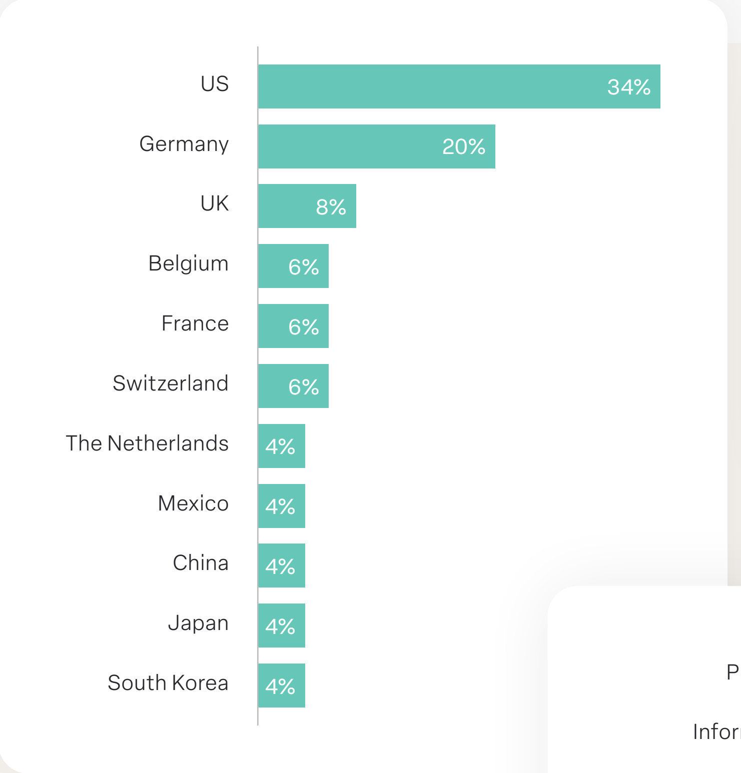


Figure 19: Company's HQ Location

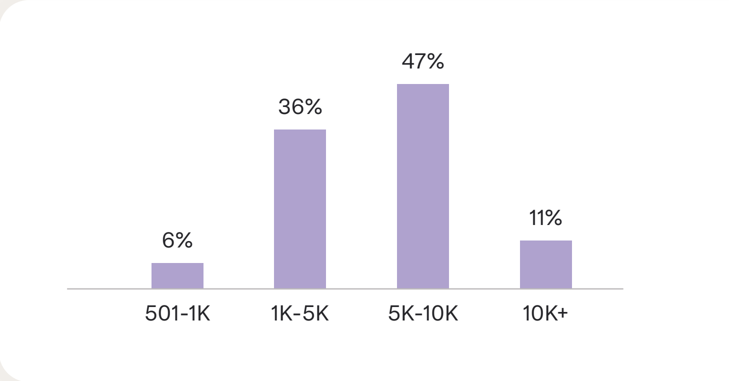


Figure 20: Company Size

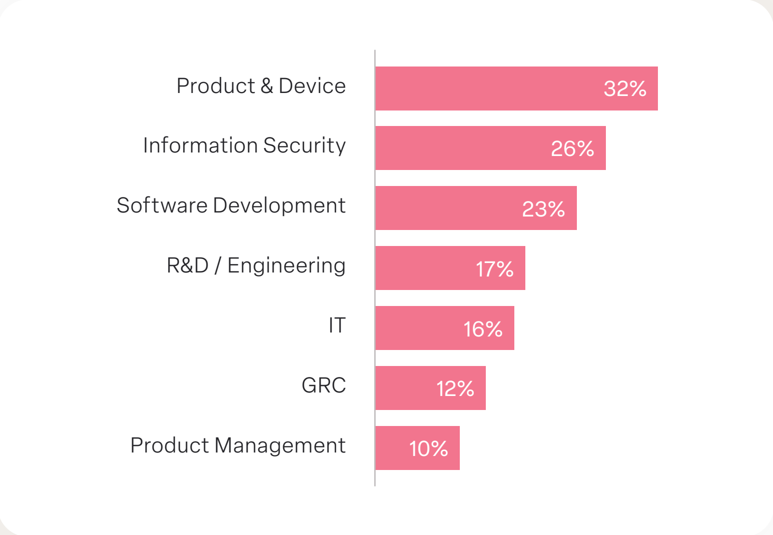


Figure 22: Areas of Work

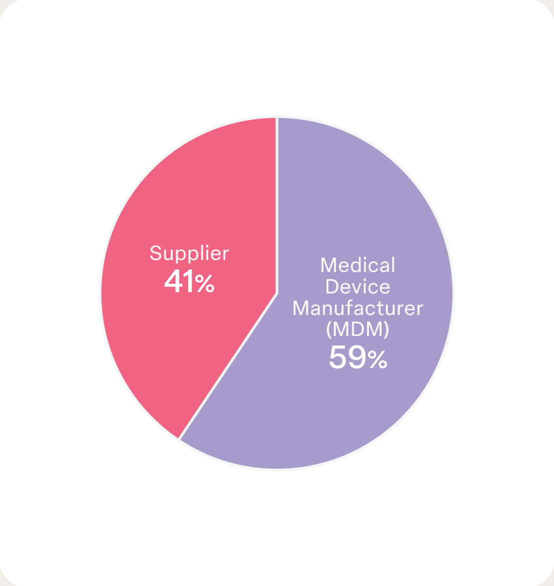


Figure 21: Role in Medical Device Industry

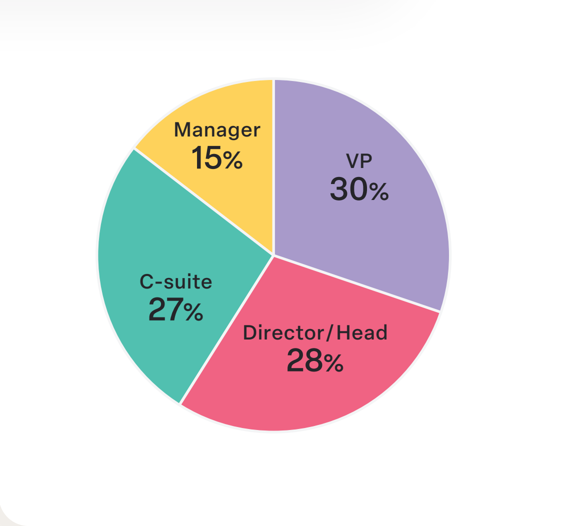


Figure 23: Job Seniority

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Device manufacturers such as Danaher, Supermicro, LG Electronics and Drager use Cybellum's Product Security Platform and Professional Services to manage the main aspects of their cybersecurity operations across business units and lifecycle stages. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Learn More

Follow us for news and updates cybellum.com