CYBELLUM

2023 Medical Device Security Survey Report

November 2023

Table of Contents

Introduction & Key Findings

Introduction & Methodology

The healthcare landscape is in a critical phase where the security of medical devices has taken center stage for all Medical Device Manufacturers (MDMs). As medical devices continue to evolve into software-driven machines, the challenge of staying ahead of cybersecurity risks becomes even more complex. The expanding attack surfaces, proliferation of vulnerabilities, and intricate supply chains make it increasingly difficult to maintain the security and compliance of the entire product portfolio at all times.

This critical moment for medical device security is underlined by several key developments in the field. First, the Omnibus bill that went into effect in March of this year, has cast a spotlight on medical device security, emphasizing the need for enhanced safeguards. This legislation has ignited a profound shift in the healthcare sector's approach to device cybersecurity, such as the FDA's Refuse to Accept (RTA) policy for medical devices that don't meet minimum product security standards.

The FDA, the regulatory authority overseeing medical devices in the USA, has clearly communicated its commitment to scrutinizing device approval submissions. The agency is actively engaged in investigating over a dozen security issues related to MDMs and their devices, indicating a growing emphasis on security within the industry. They have also recently published their latest premarket cybersecurity guidelines while simultaneously delving into postmarket security maintenance, recognizing the need for comprehensive security throughout a device's lifecycle.

Moreover, recent findings from the Health Information Sharing and Analysis Center (Health-ISAC) underscore the rising threat landscape that the healthcare industry is facing. A recent survey by Health-ISAC revealed a startling 59% year-over-year increase in vulnerabilities within medical devices and products in 2022. This data serves as a stark reminder of the escalating cyber risks facing the medical device industry.

It is in light of these critical challenges and developments that we initiated this follow-up to our 2022 Medical Device Security survey. Our objective is to gain a deep understanding of how the medical device industry has evolved over the past year concerning device security. By identifying the main challenges and gaps that MDMs currently face, we aim to shed light on the path forward for a more secure and resilient medical device landscape.

Methodology

Our survey, conducted in September 2023, targeted 150 full-time employees in the medical device manufacturing industry. Respondents were from the USA, Germany, the Netherlands, Belgium, the UK, Switzerland, Japan, Mexico, Denmark, France, South Korea, and Canada.

We specifically focused on individuals with titles in Product Security and Cybersecurity Compliance within companies with 500 or more employees. Our survey was distributed via email through a global B2B research panel in collaboration with Global Surveyz, an independent survey company.

Key Findings

1

Medical device security programs remain immature

Despite an improved stance on medical device security, only 32% of respondents believe their organizations have mature device security programs. This immaturity is reflected in organizations' lack of confidence in addressing post-market incidents, with only 15% of respondents being very confident in their ability to handle cyber risks in a timely manner once devices are on the market. It is also further illustrated by the findings that 72% of companies lack a dedicated product security function, even while 33% acknowledge the need to enhance product security management and governance. It's worth asking how MDMs can effectively drive security initiatives in the absence of dedicated leadership in this crucial domain.

2

Streamlining work with R&D emerges as the top device security challenge

The top device security challenge for 2023 is establishing frictionless product security processes with R&D, chosen by 33% of respondents. Following closely are continuous product security management throughout a device's lifespan (32%) and addressing the increasing number of tools and technologies involved in product security (29%). Comparing these findings with those from 2022, it is evident that MDMs are maturing in their understanding of the intricate field of product security. They now face practical challenges they may not have encountered before, including the need to expand teams (last year's bottom priority) and improving operational efficiency.

3

Reducing time to remediation is a top priority

We see significant changes in MDMs' device security priorities from 2022 to 2023. Reducing the time to remediate vulnerabilities has taken the lead, rising from fifth place in 2022. Improving compliance has also gained significant importance, moving up from the third-place position. In contrast, shifting left product security has slipped from its top rank to third.

This adjustment in priorities suggests that MDMs may have missed opportunities for automation and expediting security processes, as we see that increasing headcount has become a higher priority while replacing manual processes with automated ones remains the lowest priority. Additionally, this shift may also be a response to the mounting volume and complexity of cybersecurity risks associated with medical equipment.

In addition to these concerns, MDMs are also prioritizing facilitating SBOM management and establishing incident response teams, underscoring their commitment to well-established best practices that offer clear business value while reinforcing compliance efforts.

4

50% of MDMs increased their device security budgets in 2023

Medical device manufacturers persist in their investments in medical device security. In 2022, 99% of companies raised their budgets with a weighted average increase of 29%. In 2023, 50% of surveyed companies increased their device security budgets by an average of 17%, while the remainder maintained their budget levels. This more measured budget growth may be attributed to previous high investments and potential impacts of the global economic climate.

Compliance with regulations, standards, and guidelines is on the rise

Medical device manufacturers are displaying an increased commitment to compliance with regulations, standards, and guidelines, responding to heightened scrutiny from legislators and regulators regarding medical device security. Our survey found that compliance rates have risen significantly compared to last year, underscoring MDMs' recognition of this issue as a top priority in our 2022 survey. As a testament to their dedication, MDMs' 2023 compliance plans project an impressive achievement of over 95% compliance with various regulations and standards. This proactive stance showcases MDMs' efforts to meet the evolving requirements and expectations surrounding medical device security.

5

Survey Findings

Attitude Towards Device Security

Overall, we see a significant change in mindset within the medical device industry. 92% of respondents strongly agree that device security plays a crucial role in minimizing business risk (up from 79% in 2022).

The change is most dramatic in the context of "negative" statements. For example, the perception that device security is a "necessary evil" imposed by regulators decreased dramatically from 80% in 2022 to 44% in 2023. Similarly, the practice of doing the minimum for compliance dropped from 78% in 2022 to 26% in 2023. The belief that getting products to market takes precedence over device security plummeted from 79% in 2022 to 14% in 2023, highlighting a growing realization among MDMs that device security can no longer be sidelined.

These findings illustrate a critical shift in the perception of the importance of device security, prompting us to ask, "Will this newfound understanding lead to tangible improvements in medical device security practices?"

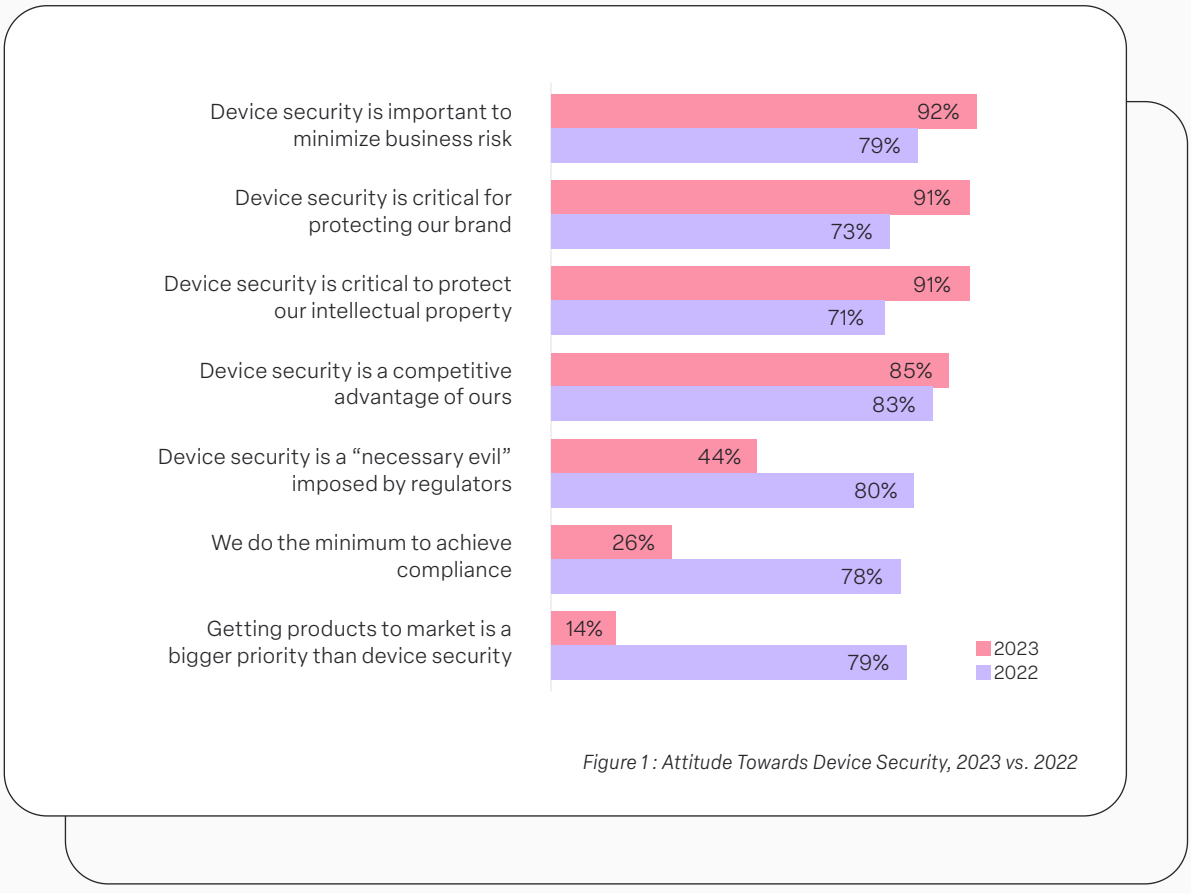


Figure 1 : Attitude Towards Device Security, 2023 vs. 2022

Product Security Program Maturity Level

Our survey offers valuable insight into the maturity levels of medical device security programs among respondents.

The responses showed the following breakdown:

- 19% of the participants reported their company's security program at Level 1, Firefighting. Notably, smaller companies with fewer than 5,000 employees (23.1%) were more likely to be in this firefighting state compared to larger organizations with over 5,000 employees (7.1%).
- 49% of respondents indicated that their organizations operate at Level 2, Passive Defense, reflecting a more proactive stance compared to Level 1, but still not achieving FDA readiness.
- A mere 32% of participants stated their companies were at Level 3, FDA Ready, representing the highest level of maturity aligned with the expectations outlined by regulatory bodies such as the FDA.

As we can see, the clear majority, 68% of respondents, expressed that their programs are currently below the desired maturity level. This indicates that a substantial amount of work remains to be done to enhance the overall maturity and effectiveness of medical device security programs across the industry.

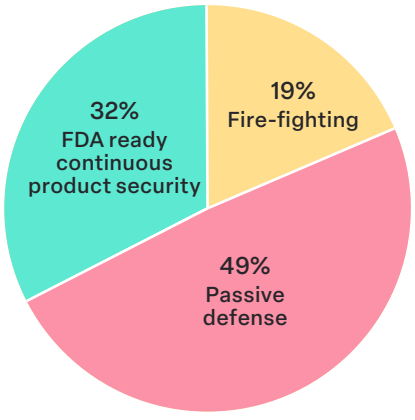


Figure 2 : Product Security Program Maturity Level

Level 1 - Fire-fighting: Product security processes are unorganized, security scans are performed just at the end of development, highly manual work, major compliance gaps, no threat or device monitoring post production. Success relies on individual efforts, and isn't repeatable. Time-to-Market suffers.

Level 2 - Passive defense: Partially defined processes with few assigned dedicated resources. Basic product security practices are implemented periodically using disconnected generic or homegrown tools, with plenty of manual work. Compliance improves, but is inconsistent. Time-to-Market is at risk and there are security gaps post production.

Level 3 - FDA ready continuous product security: Resources are available at the executive and practitioner level. A dedicated process is in place with a high degree of automation for both product security and compliance activities, covering the entire product portfolio from design to post production. Products get to market much faster and stay there, while minimizing risk.

Confidence in Addressing Post Market Security Incidents

A significant 70% of survey respondents expressed confidence in their ability to effectively mitigate post- market cyber risks in medical devices in a timely manner, with 15% being “very confident” and 55% “somewhat confident.” This reflects a collective belief in their organizations' capacity to address security challenges once devices are in circulation.

In contrast, 30% of respondents expressed being "not very confident" or "not confident at all".

Interestingly, the level of confidence in managing post-market cyber risks varies by region, with the highest confidence levels observed in the USA (84%) compared to 67% in Germany and 61.4 % in the Rest of the World (ROW).

Unsurprisingly, the data indicates a strong correlation between maturity levels and confidence in post-market incident response capabilities. Level 1 maturity companies, which are still in a firefighting state, showed the lowest confidence, with only 3.6% expressing some level of confidence. In contrast, more mature Level 2 companies exhibited 77% confidence, and Level 3 companies, characterized by FDA-ready continuous product security, displayed 100% confidence in their post-market incident response capabilities.

The results underscore a clear trend: higher device security program maturity correlates with increased peace of mind regarding post-market incident response capabilities.

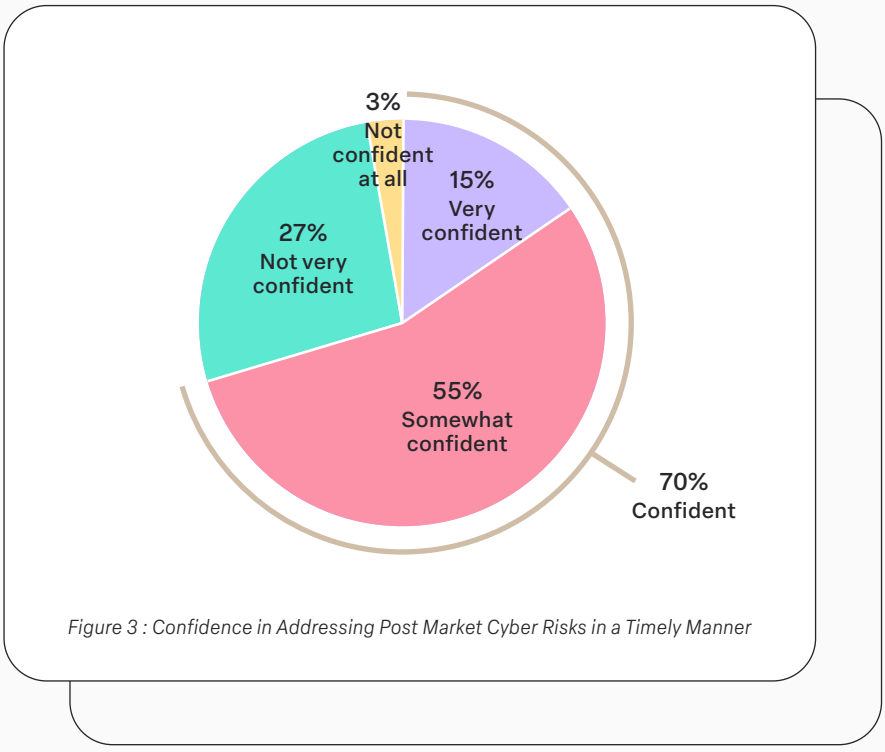


Figure 3 : Confidence in Addressing Post Market Cyber Risks in a Timely Manner

Organizational Ownership for Medical Device Security

We found that the key roles responsible for medical device security are the Chief/VP/Head of Product Security (28%), Chief/VP/Head of Compliance or GRC (19%), and Chief Information Security Officer (CISO) (17%).

Compared to our 2022 survey, there have been slight changes in ownership. The Chief/VP/Head of Product Security's role increased from 25% to 28%. Similarly, the Chief/VP/Head of Compliance or GRC's role in product security ownership rose from 14% to 19%. In contrast, ownership by the CTO dropped from 25% to 12%.

Of note, we found that companies located in Germany are more likely to have the CISO responsible for device security (30%) than other regions (14%). The same holds true for suppliers (27%) compared to OEMs (13%), across all regions.

Overall, despite improved attitudes toward medical device security, 72% of surveyed MDMs still lack a dedicated function for product security, highlighting the overall immaturity of product security programs in these organizations.

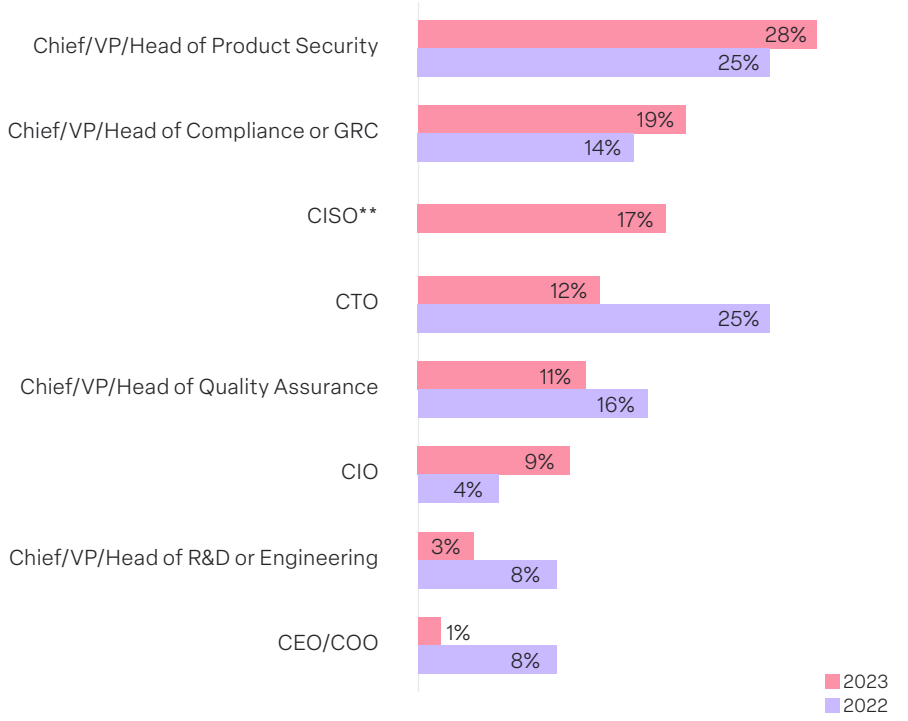


Figure 4 : Organizational Ownership for Medical Device Security

**Question not asked in 2022

Top Medical Device Security Challenges

The most pressing device security concerns for 2023 include establishing frictionless product security processes with R&D (33%), continuous product security management throughout a device's lifespan (32%), and the evolving landscape of tools and technologies (29%).

Comparing these findings to our 2022 survey, it's evident that MDMs are gaining a deeper understanding of product security. However, it also reveals that they face new practical challenges, such as streamlining R&D processes, which has risen from a low rank in 2022 to a top concern in 2023. The need to expand security teams, a low-ranking issue in 2022, has also now gained importance.

Interestingly, tracking the resolution of security issues is the lowest priority overall, but significantly more critical for suppliers (31.8%) compared to OEMs (18.9%), indicating a bottom-up challenge rather than a top-down one.

Overall, the multitude of challenges across different categories with similar weightage highlights the complexity of device security. With 68% of companies' programs lacking maturity, it's no surprise that organizations grapple with multiple challenges simultaneously, underscoring the pressing need for improvement.

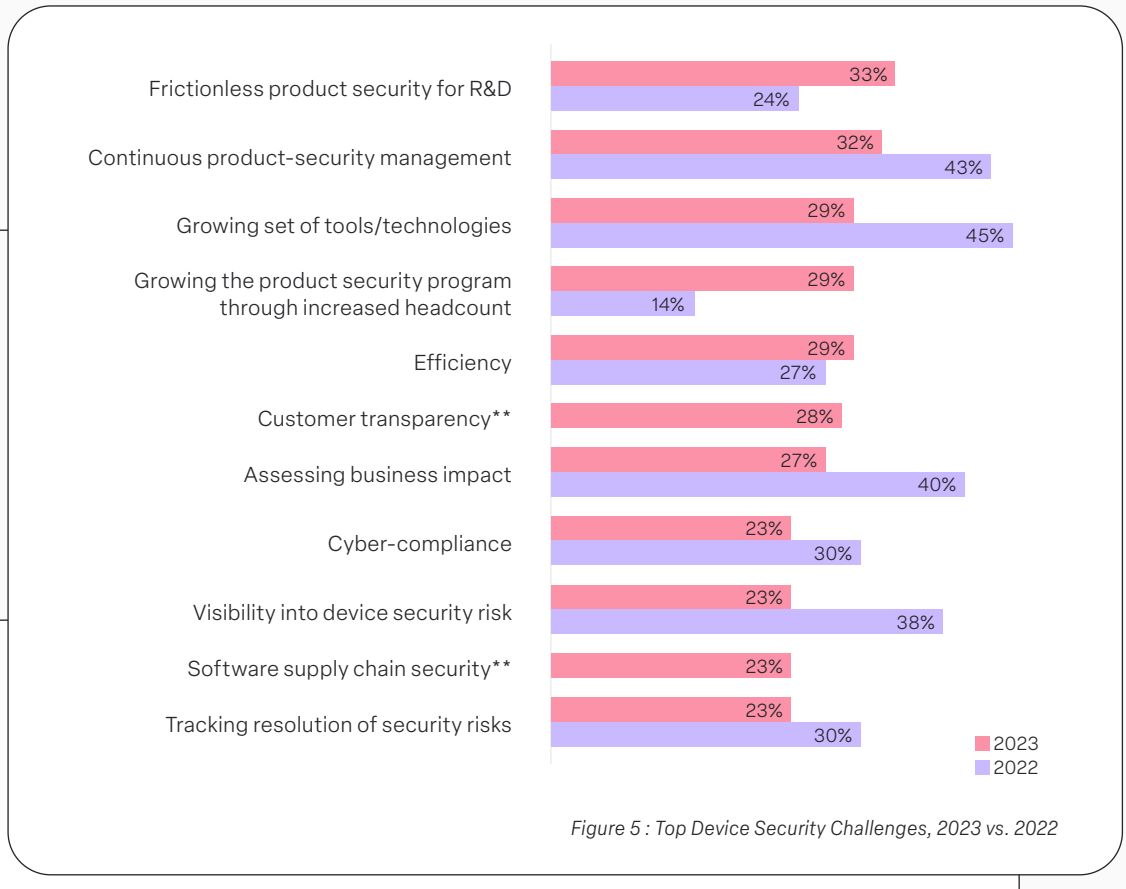


Figure 5 : Top Device Security Challenges, 2023 vs. 2022

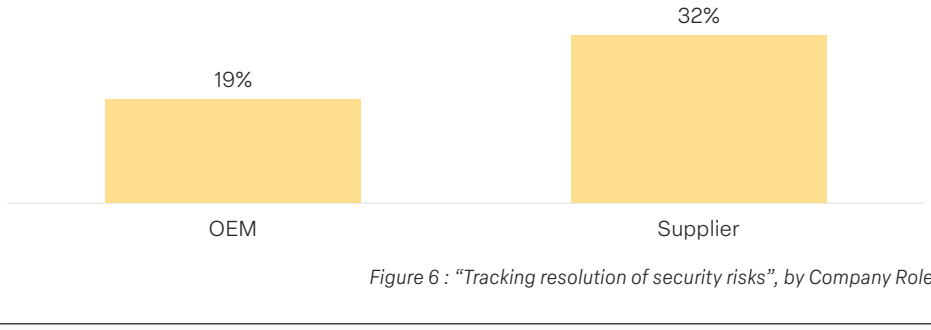


Figure 6 : "Tracking resolution of security risks", by Company Role

*Question allowed more than one answer and as a result, percentages will add up to more than 100%
**Question not asked in 2022

Top Priorities for Product Security Roadmap

The primary focus for MDMs in 2023 centers on the following priorities:

- Reducing time-to-remediation of vulnerabilities (28%): A significant shift from 2022, as this priority now claims the top spot compared to ranking 5th last year.
- Improving compliance submission success rate (27%): While this remains a significant concern, it has decreased from 34% in 2022.
- Integrating security earlier in the design development stage (26%): A continuing emphasis on security by design, although it has decreased from 37% in 2022.

The surge in prioritizing reducing time-to-remediation may reflect the growing complexity and volume of vulnerabilities. This is evidenced by the growing priority of increasing headcount (20% in 2023, up from only 4% 2022), indicating a strategic shift in approach.

While software supply chain security has dropped in the rankings, it remains a high priority in the USA compared to other regions.

We also note that there is a missed opportunity to leverage automation for expedited device security processes. Despite the need for efficiency, replacing manual processes with automated ones ranks lowest in priorities. This discrepancy suggests a potential oversight in harnessing technology to address the escalating challenges.

The industry's commitment to other crucial aspects, including SBOM management (24%), incident response (23%), and overarching management and governance (21%), remains aligned with established best practices and regulatory guidance, such as that provided by the FDA.

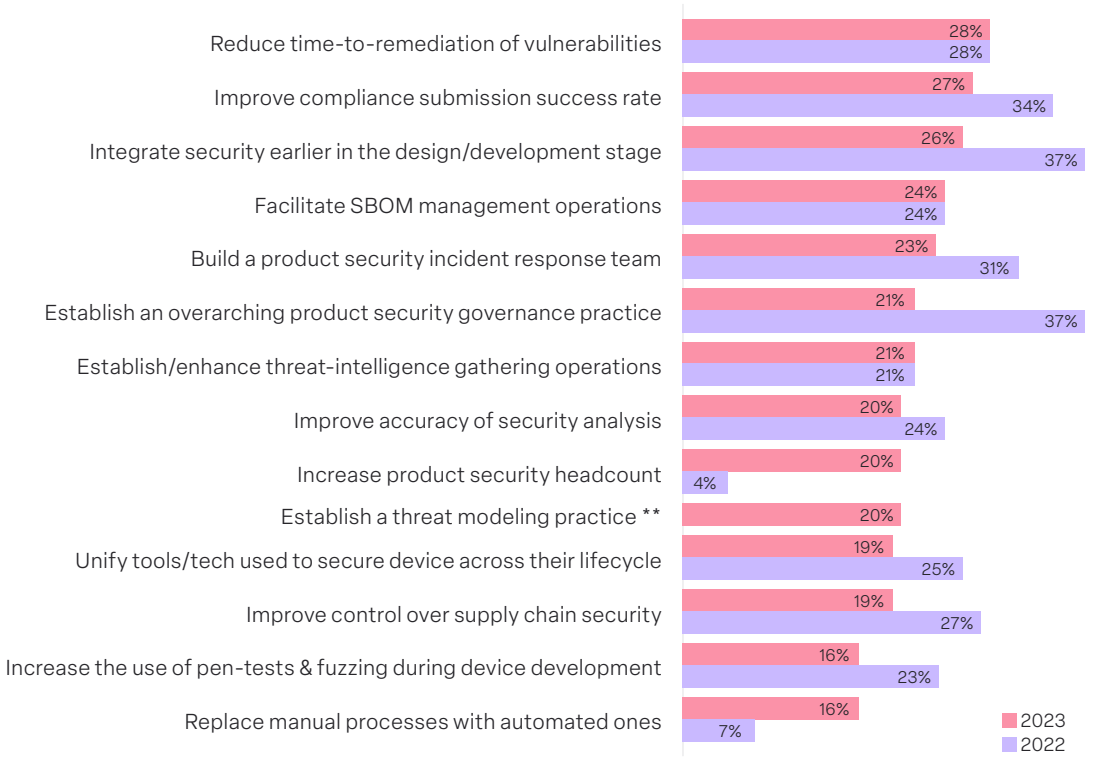


Figure 7 : Top Priorities for Product Security Roadmap, 2023 vs. 2022

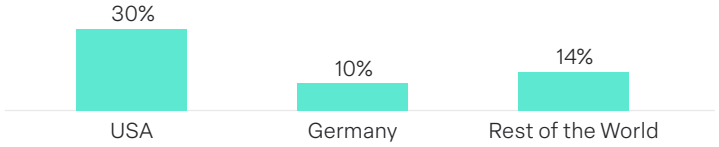


Figure 8 : "Improve control over software supply chain cybersecurity", by Country

*Question allowed more than one answer and as a result, percentages will add up to more than 100%
**Question not asked in 2022

Complying With Medical Device Cybersecurity Regulations, Standards, and Guidelines

MDMs demonstrated higher compliance rates with cyber regulations and guidelines in 2023 compared to 2022. The top three regulations adhered to include IMDRF (72%), EU Guidance (69%), and FDA Postmarket Cybersecurity Management (62%).

There are some noteworthy findings within the compliance landscape:

- Level 3 maturity companies demonstrate significantly higher compliance with the FDA's Postmarket Cybersecurity Guidance (73%) compared to their less mature counterparts (56%).
- Larger companies show greater compliance with the NTIA's SBOM Critical Elements (85.7%) and the EU MDR/IVDR (92.9%) compared to smaller ones. However, larger companies lag behind in compliance with the FDA's Premarket guidance (47.6%).

These findings align with the priorities set by MDMs in 2022 and the increased legislative and regulatory pressure in the medical device industry in 2023.

Noteworthy is the industry's commitment to compliance as reflected in future plans for 2023. If we incorporate MDMs' 2023 compliance plans, the industry achieves an impressive & 95% compliance with all regulations, demonstrating a commitment to meet evolving standards and regulations.

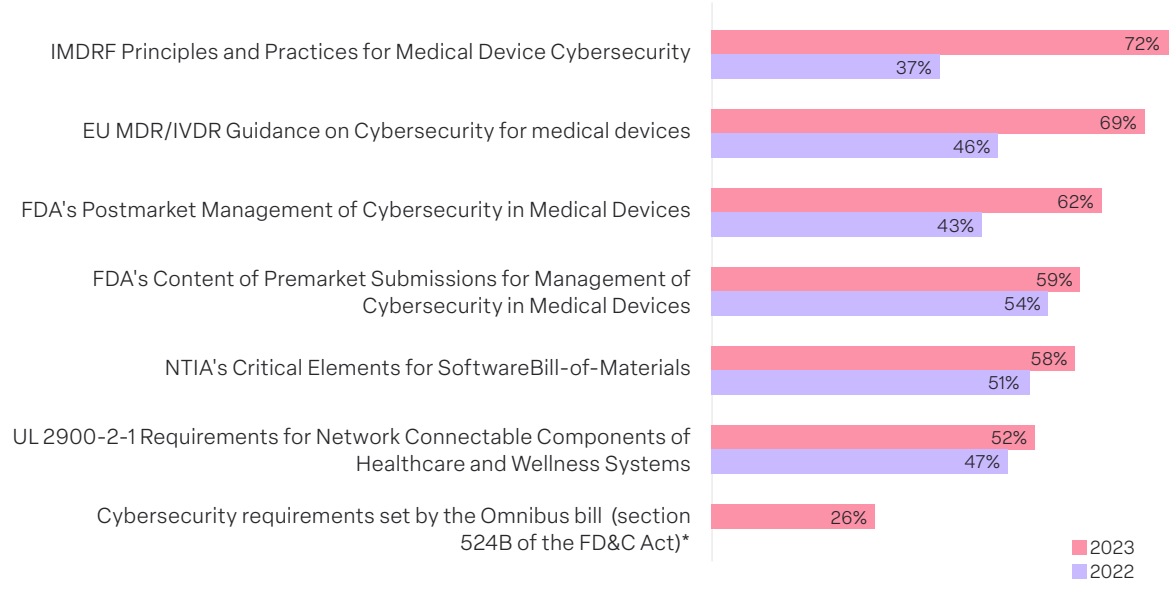


Figure 9 : Compliance with Medical-Device Security Regulations, 2023 vs. 2022

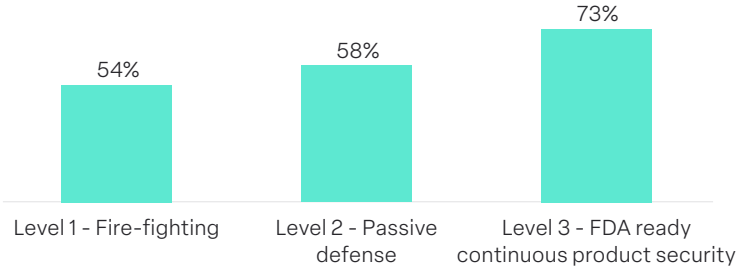


Figure 10 : Complying with the FDA's Postmarket Cybersecurity Guidance in 2023, by Product Security Maturity Level

*Question not asked in 2022

Product Security Budget Changes

According to our survey, 50% of respondents reported an increase in their device security budgets in 2023, while 49% mentioned that their budgets remained unchanged, and only 1% reported a decrease. The average increase in the product/device security budget was 17%.

In comparison, our 2022 survey found that 99% of companies planned to increase their budgets with a weighted average growth rate of 29%.

This indicates that medical device manufacturers continue to invest in device security, with a YoY budget increase, although at a lower growth rate than the previous year.

A closer look at the data reveals two key insights:

- Budget increases were more prevalent in companies with mature product security programs, both at Level 2 and Level 3 (around 53%), compared to those with immature security programs (32.1% for Level 1).
- US-based companies exhibited a higher propensity to increase their budgets compared to their counterparts in other regions.

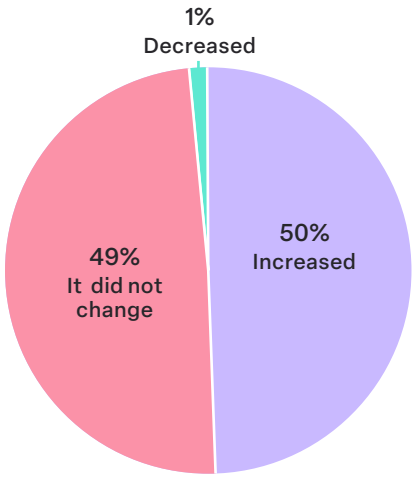


Figure 11 : Product Security Budget Changes

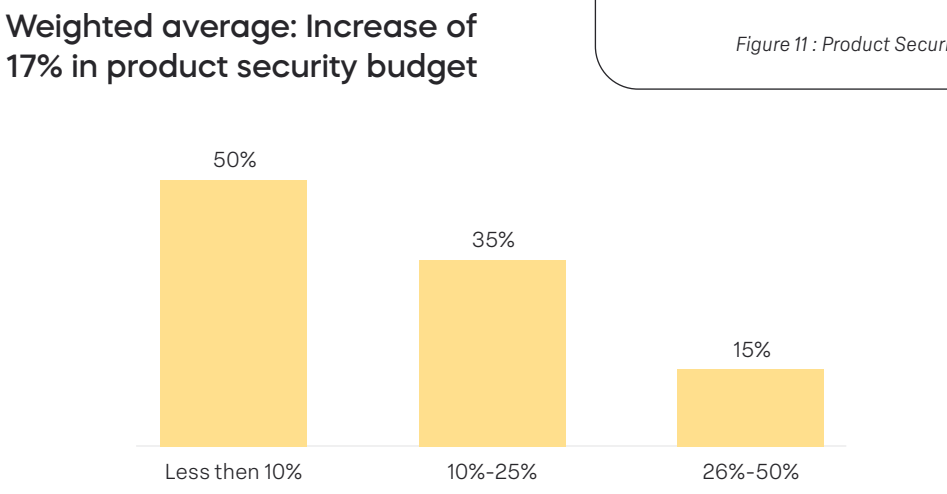


Figure 12 : Increase of Product Security Budget

Common Practices Used to Address Software Supply Chain Security Risks

Medical device manufacturers have implemented various practices to address supply chain security effectively. The top practices include:

- Tracking security performance KPIs for suppliers (87%) such as time to respond to requests, time to close tickets, and number of detected vulnerabilities per delivered component
- Maintaining an up-to-date database of Software Bill of Materials (SBOMs) (77%)
- Generating and sharing SBOMs for products (70%)

Notably, original equipment manufacturers showed a greater inclination for generating and sharing SBOMs compared to suppliers.

Additionally, the Vulnerability Exploitability Exchange (VEX) is emerging as a method to communicate vulnerability status across the supply chain, albeit with lower adoption numbers, likely due to its relatively recent introduction.

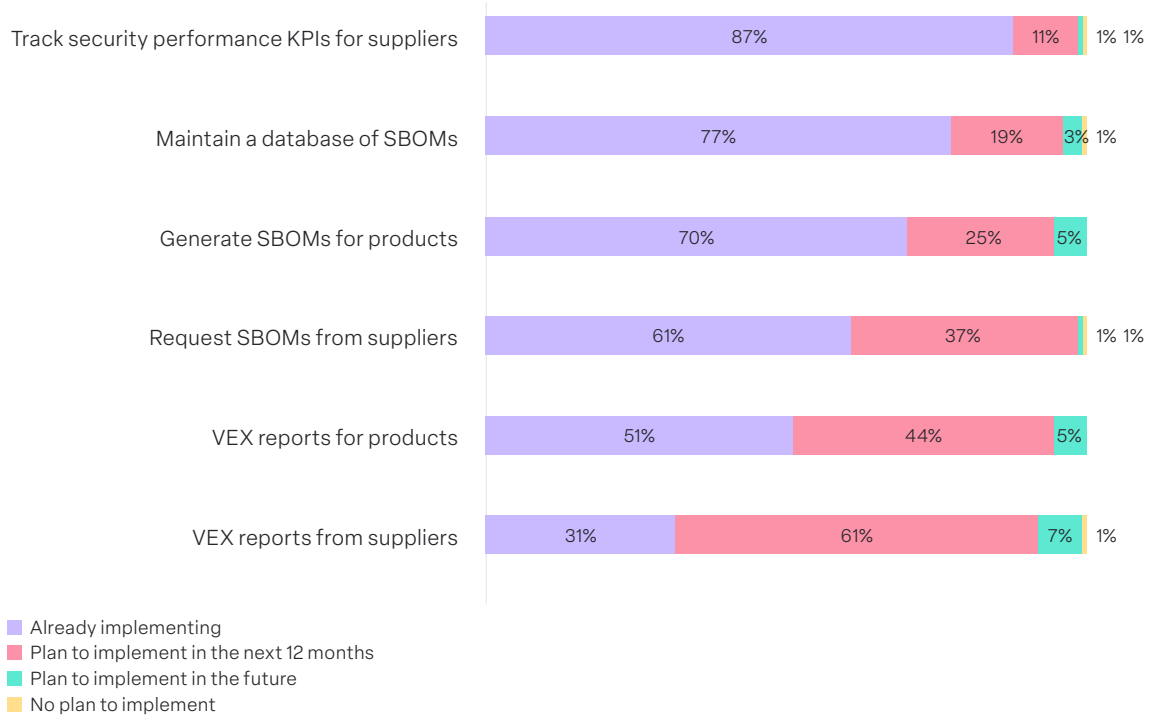


Figure 13 : Common Practices Used to Address Software Supply Chain Security Risks

Product Security Practices Requiring Improvement

We found that the top three practices respondents ranked as most requiring improvement at their companies were:

- Incident response (39%)
- Cyber-compliance readiness (37%)
- Threat modeling (35%)

Comparing 2023 data to 2022, the top five product security practices requiring improvement have slightly shifted. Incident response, cyber-compliance, and threat modeling now lead the list. Threat modeling, which ranked sixth in 2022, has risen to the third spot in 2023. These are closely followed by overall product security management and governance, with Software Bill of Materials (SBOM) management slipping from the top spot in 2022 to the fifth spot in 2023.

These shifts align well with the priorities outlined by the FDA, indicating that medical device manufacturers are seeking to enhance their practices in these areas.

It's essential to recognize that respondents provided diverse answers, reflecting gaps in various aspects of product security across organizations, emphasizing the complex and multifaceted nature of the field.

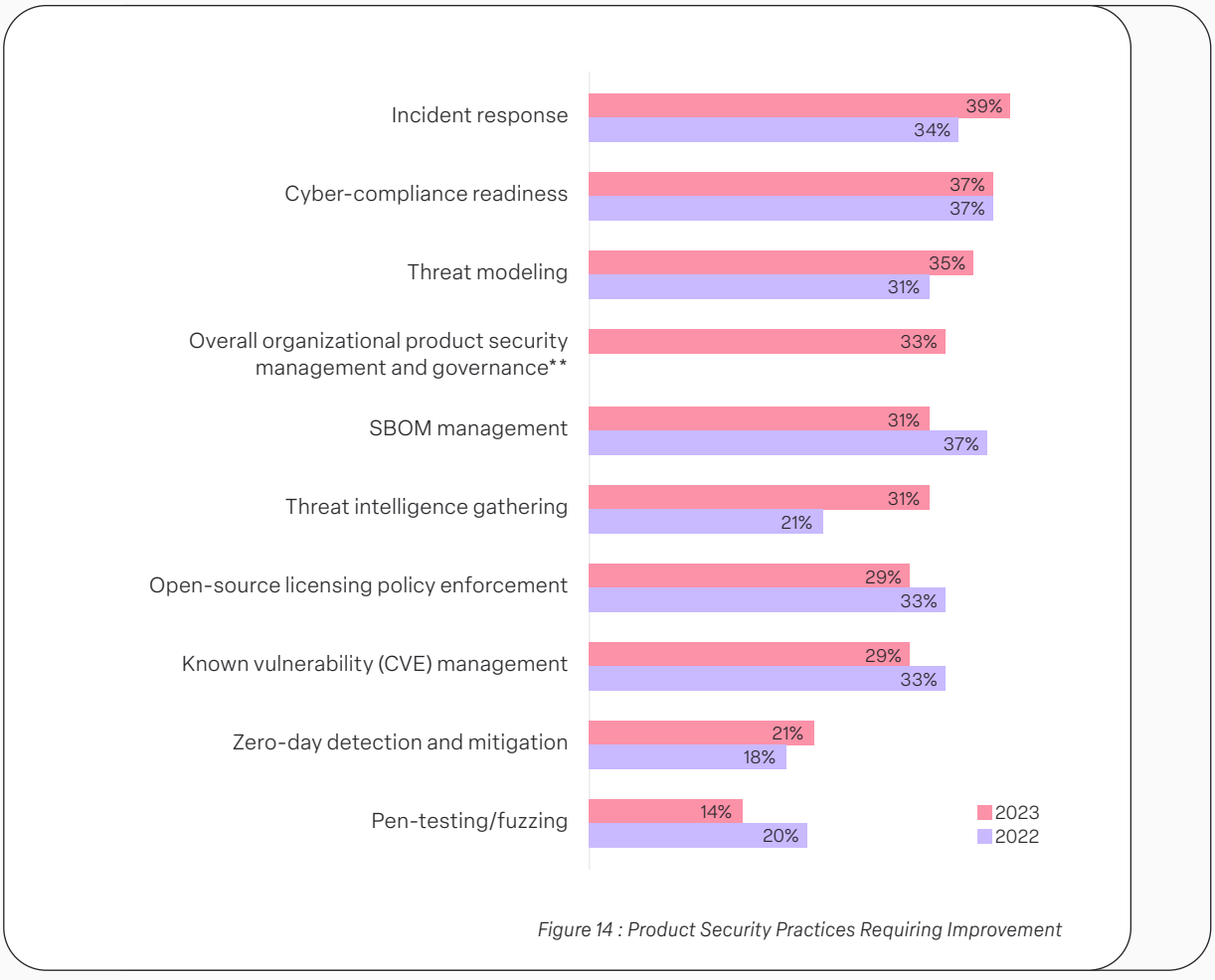


Figure 14 : Product Security Practices Requiring Improvement

*Question allowed more than one answer and as a result, percentages will add up to more than 100%
**Question not asked in 2022

Demographics

Country, Company's Role in MDI, Company Size, Areas of Work, and Job Seniority

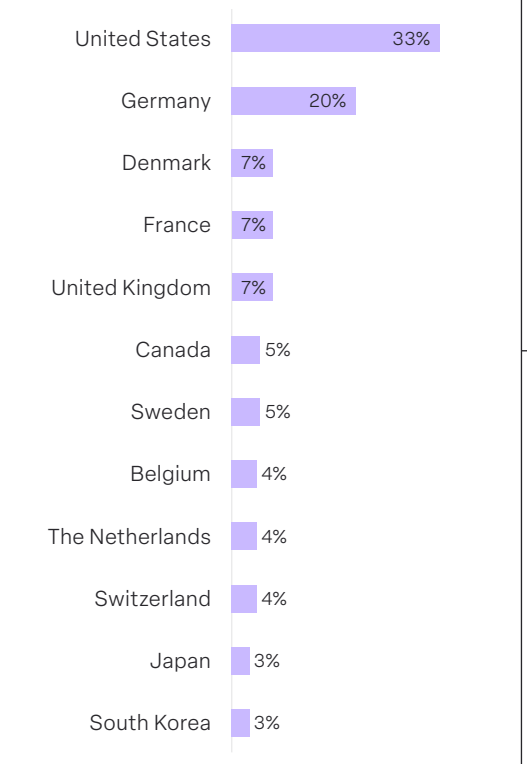


Figure 15 : Country

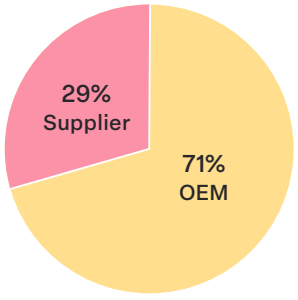


Figure 16 : Company Role

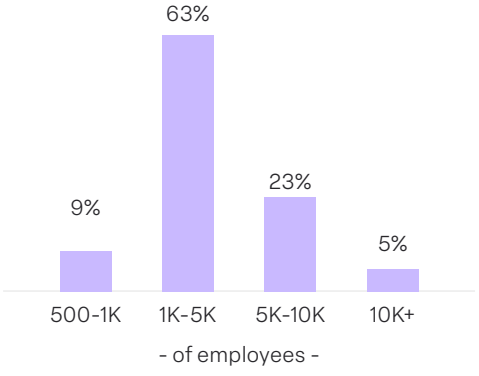


Figure 17 : Company Size

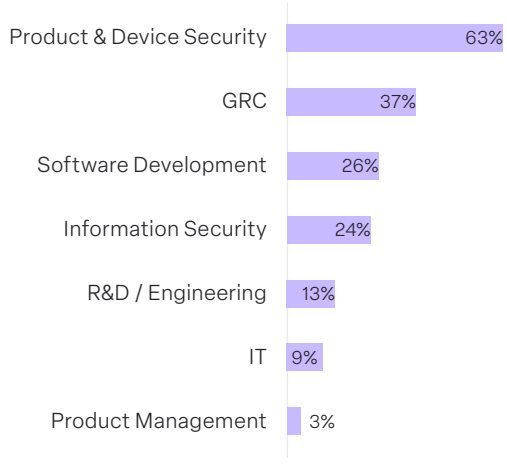


Figure 18 : Areas of Work

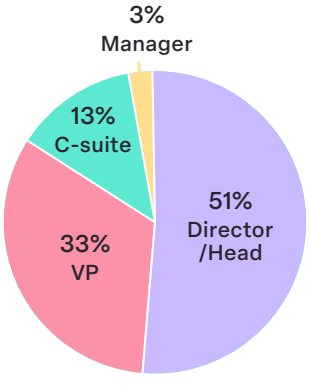


Figure 19 : Job Seniority

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Top medical device manufacturers such as Danaher and Siemens use Cybellum's Product Security Platform and services to manage cybersecurity risk and FDA compliance across business units and lifecycle stages. From SBOM to Vulnerability Management, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Experience what product security can be. Book a demo.

Learn more about Product Security

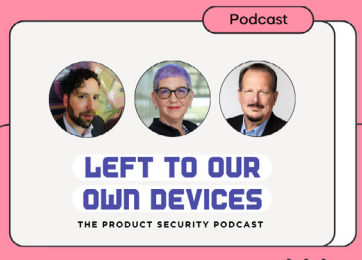
Blogs

Introduction to Medical Device Security Standards and Regulations

Rolling Regulations: Embrace Them, Don't Chase Them

How to Keep the Software Supply Chain Accountable with SBOMs

Podcasts



Knowledge Base

Breaking down the FDA's 2023 Premarket Cybersecurity Requirements

Learn More →

How Medical Device Makers Can VEX Cyber Threats and Secure the Healthcare Supply Chain

Learn More →

SBOM for Connected Devices: Getting it Right

Learn More →

More about the Product Security Platform