2023 Product Security Annual Report

Cybersecurity by design,
in use and through partnership

BD
Advancing the world of health™

Innovation. Security. Trust.

For more than 125 years, BD has been *advancing the world of health*™ by creating new technologies. We maintain a culture of transparency and continually strive to improve the security of BD products to help protect patient safety and privacy. Our R&D scientists and engineers, in close partnership with colleagues across Product Security, Cybersecurity, Quality, Regulatory and Privacy, share a passion for innovating to make a difference. As we seek to address some of the most pressing healthcare challenges, we strive to provide secure and reliable healthcare technologies to advance care across the patient journey, today and into the future.

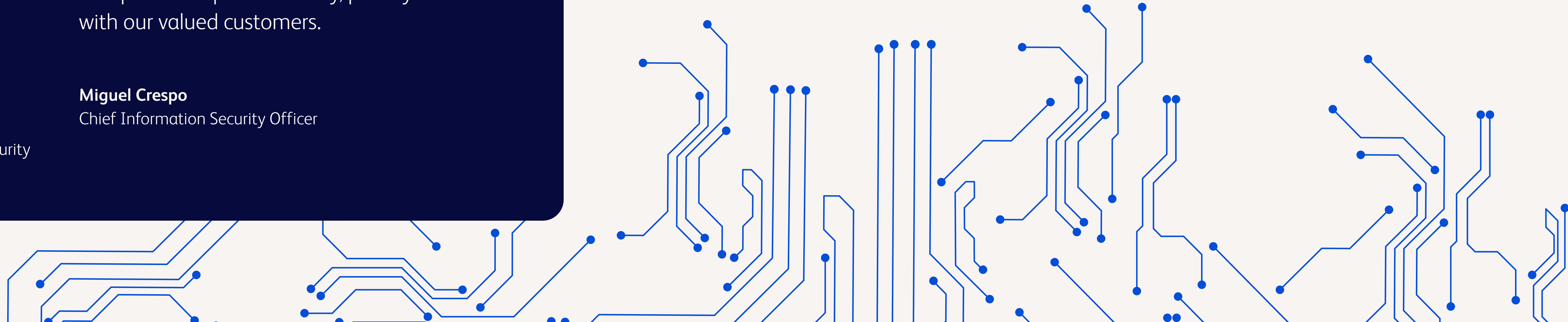
Nimi Ocholi
Vice President, Research and Development, Product Security

At BD, cybersecurity is deeply ingrained in the fabric of our organization. Our enterprise Cybersecurity and Product Security teams collaborate closely to help safeguard our products, customers and patients. By strengthening our systems, prioritizing data protection, refining our cybersecurity protocols and fostering a cyber-smart culture across our global enterprise, we enhance our ability to create and maintain secure medical technologies. This collaborative approach not only bolsters cybersecurity and resilience but also prioritizes patient safety, privacy and trust with our valued customers.

Miguel Crespo
Chief Information Security Officer

The state of healthcare cybersecurity

Globally, cyberattacks continue to increase in sophistication, frequency and intensity. Organizations across all industries must be vigilant and proactive to protect against and respond to cybersecurity risks. For healthcare, the potential impact of cyberattacks goes beyond disruption to the availability, confidentiality and integrity of systems and data. Patient care can be impacted when medical devices or systems become unavailable or cannot be trusted due to cyberattacks, or when such attacks cause interruptions or delays. To protect patient safety and privacy, healthcare delivery organizations, medical device manufacturers and third-party suppliers must work together to guard against cybersecurity risks. By working to secure BD products, we are helping to protect the healthcare ecosystem.



Healthcare cybersecurity trends

Three cybersecurity trends have impacted the healthcare industry over the last year:

Cyberattacks are becoming more frequent, advanced and adaptive.

Increased reliance on digital infrastructure and systems, coupled with emerging technologies like artificial intelligence and robotic process automation, are providing new avenues for threat actors to launch cyberattacks. In healthcare, the top motivation behind cyberattacks is financial gain[1]. The U.S. Department of Health and Human Services (HHS) tracks large data breaches through its Office for Civil Rights. Between 2018 and 2022, large breaches in the U.S. increased 93% and large breaches involving ransomware increased 278%[2]. Geopolitical events have also increased cybersecurity risks on a global basis.

Artificial Intelligence (AI)-enabled cyberattacks are changing the threat landscape.

In August 2023, HHS issued a warning about ransomware attacks being launched via phishing emails[3]. Around the same time, malicious generative artificial intelligence (GenAI) tools like WormGPT and FraudGPT began to emerge on the dark web, making it even easier for threat actors to plan and launch these types of attacks[4]. In addition, Gartner® predicts that "By 2025, the consumerization of AI-enabled fraud will fundamentally change the enterprise attack surface, driving more outsourcing of enterprise trust and focus on security education and awareness[5]."

There is a collective emphasis on improving cybersecurity practices.

The entire healthcare industry is on a journey to continuously improve cybersecurity. Regulatory authorities are defining more specific cybersecurity requirements for medical devices, aimed at protecting patient safety. At the same time, cybersecurity expectations of manufacturers have increased across critical infrastructure. These changes are evident in new cybersecurity requirements for manufacturers in Japan, the United Kingdom and the United States. Practices such as managing cybersecurity over the full product life cycle, providing a software-bill-of-materials (SBOM), and communicating potential risks and vulnerabilities feature prominently in the new requirements.*

These trends reinforce the need for ongoing vigilance and continuous improvement.

At BD, our product security strategy includes a total life cycle approach to working to protect BD products and communicating with our customers and patients about potential cybersecurity risks and emerging threats. This report summarizes our approach to product security, our culture of transparency in alignment with regulatory and industry best practices, and our ongoing efforts to collaborate across the industry to advance cybersecurity in healthcare.

*For insight regarding how BD assesses emerging regulations, see page 5.

Cybersecurity at BD

Methodology

Cyberattacks are becoming more sophisticated, frequent and adaptive. No company is immune; cyberattacks can impact even the most mature technology companies. BD strives to meet high security standards. We also recognize that new cybersecurity threats emerge daily across the healthcare industry—which is why we believe transparency and collaboration are essential. We base our strategic approach to cybersecurity on three guiding principles:

Security by design

BD products are **designed with security in mind** and to align with industry-leading cybersecurity standards, including those from the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST).

Security in use

Through collaboration, BD enables customers to **secure and maintain** BD products throughout their intended useful life.

Security through partnership

BD seeks to be a **trusted partner** helping to advance cybersecurity across the industry by participating in cybersecurity working groups and public-private partnerships.

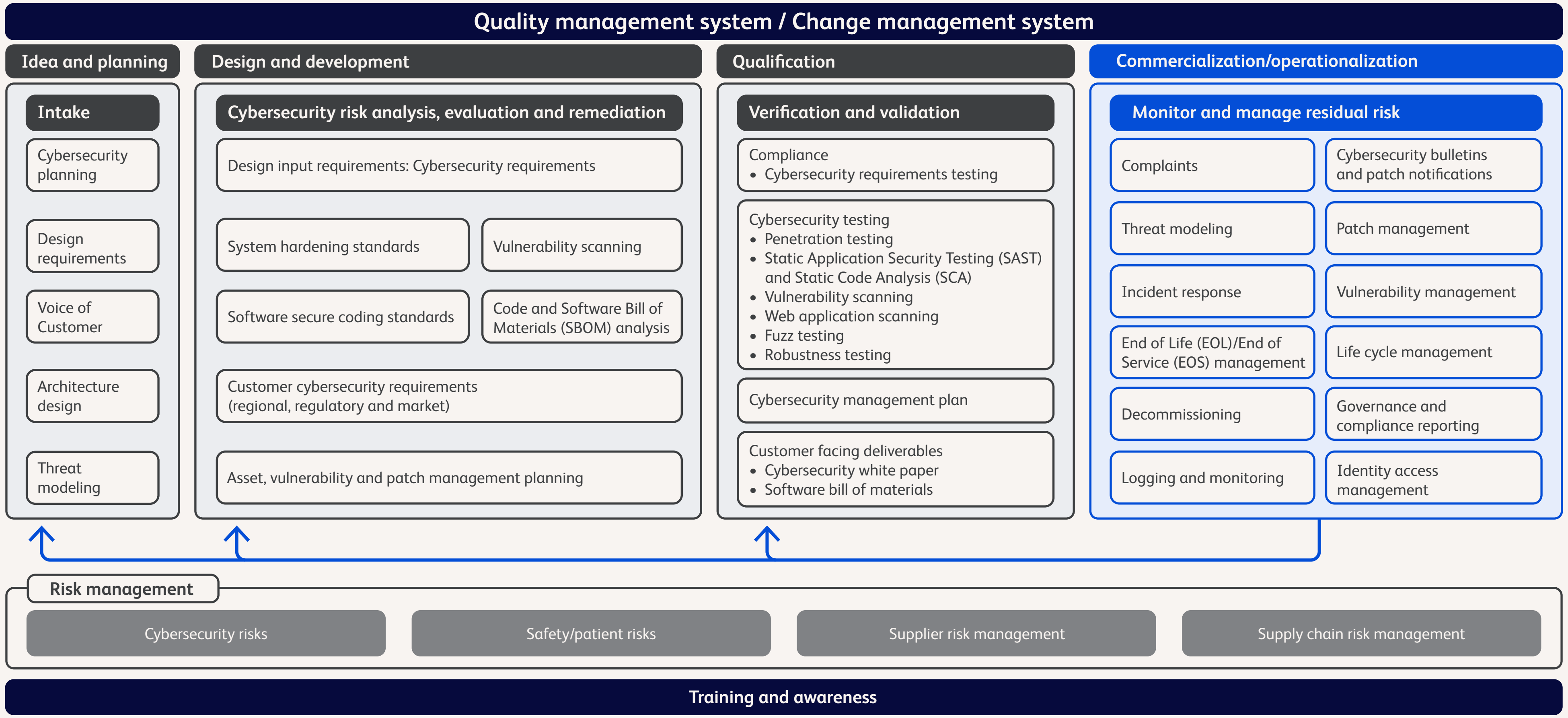
Our services

BD provides flexible servicing options for select software-enabled products. Contact your BD service representative to explore options such as patch management to augment your organization's cybersecurity capabilities.

Cybersecurity at BD

BD Cybersecurity Framework

Our Secure Software Development Life Cycle (SSDLC) follows the BD Cybersecurity Framework which incorporates design requirements, including cybersecurity risk assessment, threat modeling, penetration testing, vulnerability scanning, software composition analysis, code analysis, system hardening and continuous vulnerability management. The framework serves as a blueprint for managing cybersecurity risk across BD products. It is aligned to multiple industry standards and work products, including the Healthcare and Public Health Sector Coordinating Council (HSCC) Medical Device and Health IT Joint Security Plan, the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Underwriters Laboratories (UL) 2900 Standard for Software Cybersecurity for Network-Connectable Products.



Quality management system / Change management system

Idea and planning

Intake
- Cybersecurity planning
- Design requirements
- Voice of Customer
- Architecture design
- Threat modeling

Design and development

Cybersecurity risk analysis, evaluation and remediation
- Design input requirements: Cybersecurity requirements
- System hardening standards
- Vulnerability scanning
- Software secure coding standards
- Code and Software Bill of Materials (SBOM) analysis
- Customer cybersecurity requirements (regional, regulatory and market)
- Asset, vulnerability and patch management planning

Qualification

Verification and validation
- Compliance
  - Cybersecurity requirements testing
- Cybersecurity testing
  - Penetration testing
  - Static Application Security Testing (SAST) and Static Code Analysis (SCA)
  - Vulnerability scanning
  - Web application scanning
  - Fuzz testing
  - Robustness testing
- Cybersecurity management plan
- Customer facing deliverables
  - Cybersecurity white paper
  - Software bill of materials

Commercialization/operationalization

Monitor and manage residual risk
- Complaints
- Cybersecurity bulletins and patch notifications
- Threat modeling
- Patch management
- Incident response
- Vulnerability management
- End of Life (EOL)/End of Service (EOS) management
- Life cycle management
- Decommissioning
- Governance and compliance reporting
- Logging and monitoring
- Identity access management

Risk management
- Cybersecurity risks
- Safety/patient risks
- Supplier risk management
- Supply chain risk management

Training and awareness

BD Cybersecurity, Product Security and Regulatory teams routinely assess emerging cybersecurity regulations, rules and guidance.

These teams work cross-functionally to perform product-level gap assessments against our cybersecurity processes, and we update the BD Cybersecurity Framework accordingly as needed. For example, the BD Cybersecurity Framework was updated in 2023 to:

- Place a stronger emphasis on activities that take place during the project ideation and planning phase, including design requirements, architecture design and threat modeling.
- Clarify activities that may be carried out during the qualification phase, including verification and validation, compliance against cybersecurity requirements, and expanded activities as part of cybersecurity testing.
- Provide a more comprehensive and complete view of cybersecurity risk management, including supplier risk management and supply chain risk management.

BD anticipates updating the framework to incorporate elements of the **Medical Device and Health IT Joint Security Plan Version 2.0**, which was published in March, 2024.

Cybersecurity certifications and attestations

Cybersecurity certifications and third-party attestations provide objective assurance regarding a company's cybersecurity processes and controls. In a world where cybersecurity risks and threats are increasing, the perspective of an external, objective cybersecurity expert is highly valued.

Our certification and attestation programs include System and Organization Controls (SOC2+) and UL Cybersecurity Assurance Program (UL CAP). SOC2+ annual reports are available for multiple BD products that collect and process patient health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and other applicable laws and regulations governing the use and processing of such information. These reports are prepared by an independent third party and provide assurance regarding the operational effectiveness of BD internal controls and the security of BD products. UL CAP is another independently audited certification that demonstrates the cybersecurity of participating BD medical devices through a rigorous program of analysis.

For information about all of our cybersecurity certifications and attestations, visit the **BD Cybersecurity Trust Center**.

Cybersecurity risk assessments

BD regularly works with customers to respond to product-specific cybersecurity risk assessment questionnaires. We also participate in multiple commercially available third-party risk assessment programs to support our customers' vendor risk management processes.

Securing the medical device ecosystem

Our technology landscape continues to rapidly evolve as BD delivers significant innovations to patients and customers as we pursue our Purpose of *advancing the world of health*™. At the same time, cybersecurity risks for software and connected devices continue to grow. That is why we believe managing cybersecurity over the full product life cycle is a mission-critical initiative. This includes securing software as a medical device (SaMD), software used in medical devices and software used to make medical devices. It is not enough to release a medical device that is secure; responsible medical device manufacturers must work closely with their customers and suppliers to maintain cybersecurity over each product's intended useful life. Here is what that looks like at BD.

Products in development

BD is committed to security by design. We strive to build the latest cybersecurity best practices and advances into our products and processes from the start whenever possible. For example, our newest software-enabled products incorporate system-level threat modeling, rigorous penetration testing and code signing for authentication and code integrity. They are also designed for updateability, and their cybersecurity documentation includes a software-bill-of-materials (SBOMs).

Legacy products

The usability of a medical device often extends beyond its intended useful life. This is why communicating a clear End of Support (EOS) strategy for legacy devices is critical. At BD, we monitor end-of-life (EOL) components and tools, strategize proactive risk transfer, and provide targeted communications to keep customers informed before a product or its operating system reaches EOS.

In-market products

Securing the medical device ecosystem requires transparency and collaboration. For products in the market and in use, we prioritize ongoing vulnerability management. We do this by leveraging SBOMs for thorough, robust vulnerability monitoring and response, accelerating patch deployment, periodic penetration testing and increasing observability. When BD discovers a vulnerability in one of our products, or a potential vulnerability is reported to us and confirmed by BD, we share that information with our customers to make them aware of potential risks, mitigations and compensating controls. We do this in accordance with U.S. Food and Drug Administration (FDA) guidance and in furtherance of our culture of transparency. To learn more about our responsible disclosure processes, see Coordinated Vulnerability Disclosure Process on **page 10**.

Enabling strong cybersecurity controls

Our commitment to innovation is reflected in the products, services and solutions we develop to help advance both clinical therapy for patients and clinical process for healthcare providers. The following examples highlight some of the ways we incorporate cybersecurity controls into software releases and new product designs. The cybersecurity controls highlighted below are representative and are not intended to serve as an exhaustive list of product-related cybersecurity controls.

BD® Alaris™ Infusion System, a modular and comprehensive infusion system that includes large volume pumps, syringe pumps, patient-controlled analgesia (PCA) pumps, respiratory monitoring, dose error reduction software and electronic medical record (EMR) interoperability.

Cybersecurity enhancements include the most current Wi-Fi Protected Access with WPA3 for secure wireless communications, encryption with the latest TLS 1.3 protocol for end-to-end communications between the system server and the infusion pumps, and updates that enable the latest SHA3 certificates for Windows Server environments that enable SHA3 support.

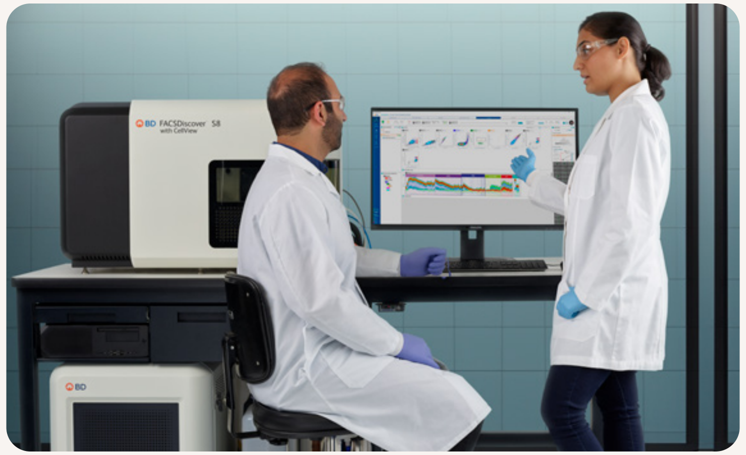
BD® Pyxis™ Enterprise Server (ES) 1.7.4, the latest software release of the Pyxis™ MedStation™ ES System, enables pharmacists to maintain a single source of truth for users and formulary, helping save time and reduce errors from manual entry.

Stronger encryption processes are enabled by default to secure customer data in transit and at rest, and software packages are digitally signed to verify their authenticity.

BD® Site-Rite™ 9 Ultrasound System, a vascular access device that provides real-time ultrasound imaging to help visualize blood vessels, needle trajectory and final tip location.

In addition to the internal penetration testing BD performs as part of product development, a pre-market version of the Site-Rite™ 9 Ultrasound System was made available to security researchers at the Biohacking Village at DEF CON 29 in 2022 for security testing purposes. Participating researchers did not report any vulnerabilities to BD. For more on the Biohacking Village at DEF CON, please see **page 12**.

Enabling strong cybersecurity controls



BD FACSDiscover™ S8 Cell Sorter*, a novel research use cell sorter designed to help researchers answer complex biological questions and discover new insights into health and disease.

The workstation is pre-installed with a third-party anti-malware solution that leverages artificial intelligence and machine learning to guard against zero-day threats.

BD® Kiestra™ Total Laboratory Automation System (third generation), a fully automated robotic track system for microbiology labs that connects different Kiestra™ modules in a flexible and customizable way and automates lab specimen processing.

Instrument PCs are set up in kiosk mode, which helps prevent unauthorized access.

BD PreVue™ II Peripheral Vascular Access System, a portable device that features real-time two-dimensional ultrasound imaging for optimized IV placement, giving patients the vascular access experience they deserve.

The system offers multiple user authentication options, including the use of a PIN, Active Directory and multifactor authentication.

For more information

Customers are encouraged to visit the **BD Cybersecurity Trust Center** to request Product Security White Papers for products they maintain. Each Product Security White Paper includes information about additional cybersecurity controls, how BD security and privacy practices have been applied, and what customers should know about maintaining security throughout each product's intended useful life.

*BD FACSDiscover™ S8 Cell Sorter is For Research Use Only. Not for use in diagnostic or therapeutic purposes. BD flow cytometers are Class I Laser Products.

Coordinated vulnerability disclosure process

BD has a mature coordinated vulnerability disclosure program to help customers manage cybersecurity risks over each product's intended useful life to support our culture of transparency.

Report

BD welcomes vulnerability reports from security researchers, customers, third-party component vendors and other external groups that wish to report a vulnerability in a BD software-enabled device. Visit the **BD Cybersecurity Trust Center** to report a potential vulnerability or security concern.

Analyze

BD partners with the issue reporter to investigate the vulnerability. If confirmed, our incident response team collaborates with various functional teams including Research and Development (which includes Product Security), as well as Quality and Privacy to respond to the issue.

Coordinate

BD follows FDA guidance to properly communicate confirmed BD product vulnerabilities in coordination with a Computer Emergency Readiness Team (CERT). We work with the Cybersecurity & Infrastructure Security Agency (CISA) to prepare coordinated vulnerability disclosures for our respective websites, and we also voluntarily report vulnerabilities unique to BD products to the FDA.

Disclose

Bulletins are published on the **BD Cybersecurity Trust Center** and the **CISA website** in a coordinated fashion. For maximum awareness, we also share BD vulnerability disclosures with Information Sharing and Analysis Organizations (ISAOs) where BD participates, including the **Health Information Sharing and Analysis Center (H-ISAC)**. H-ISAC sends hundreds of targeted alerts to its members each year from their Threat Operations Center[6]. This practice helps healthcare delivery organizations of all sizes stay current with vulnerability disclosures across the industry.

More about coordinated vulnerability disclosure

BD welcomes vulnerability reports from customers, security researchers and third-party component vendors. We also use multiple methods, including vulnerability scanning, threat modeling and penetration testing, to uncover potential risks and vulnerabilities during the design process and throughout the software development life cycle.

When a vulnerability is discovered and confirmed in a BD product, we follow FDA guidance to disclose the vulnerability so customers and/or patients can apply mitigations and compensating controls and, if a patch is available, prioritize patch management in accordance with the vulnerability severity and potential impact to patient safety and/or privacy.

When a vulnerability exists in a third-party component used in association with a BD product, BD collaborates with our third-party partners to better understand the potential impact to BD products. If BD determines that BD offerings are in scope, we issue a product security bulletin on the **BD Cybersecurity Trust Center**. Additionally, when patches are made available by third-party component vendors, we test and validate those patches before making them available to BD customers.

BD is also authorized as a Common Vulnerability and Exposures (CVE®) Numbering Authority by the CVE Program. When a vulnerability is unique to a BD device, we assign a CVE number which helps customers manage their internal vulnerability and patch management processes efficiently.

We also report the vulnerability to the FDA and work closely with CISA to prepare public disclosures that are published on the CISA website and the **BD Cybersecurity Trust Center** in coordinated fashion.

Sharing vulnerabilities in this way is an essential component to enabling healthcare providers to mitigate risks. However, we also recognize that our customers work with hundreds of medical device manufacturers, and they use Information Sharing and Analysis Organizations to stay up to date on medical device vulnerability disclosures. That is why we also share our vulnerability disclosures with the **Health Information Sharing and Analysis Center (H-ISAC)** to maximize awareness.

Vulnerability disclosure indicates maturity in an organization's cybersecurity practices. BD has led the way in this open, transparent approach and strives to help customers manage cybersecurity risks properly through awareness and guidance.

Cybersecurity resources for BD customers

BD makes numerous cybersecurity resources available to its customers via the BD Cybersecurity Trust Center, including:

- **Product Security White Papers –** BD makes Product Security White Papers available for all of its software-enabled products. These documents detail how BD security and privacy practices have been applied and provide information to educate customers about maintaining security throughout each product's intended useful life.
- **Bulletins –** These notifications, also known as vulnerability disclosures, provide product security information and recommendations related to newly discovered vulnerabilities in BD products and/or third-party components used in association with BD products.
- **Security patches –** These notifications let customers know what security patches are available and what they address. For third-party software components, BD validates all associated patches before making them available to BD customers.
- **Cybersecurity certifications and attestations –** BD makes several industry-recognized certifications and/or attestation reports for BD products available to customers.

Collaborating to strengthen healthcare cybersecurity

BD seeks to continuously learn from and contribute to the broader community of cybersecurity working groups and advocacy organizations in healthcare. BD collaborates with customers, government agencies, cybersecurity working groups, security researchers and fellow medical device manufacturers to advance cybersecurity in healthcare. This collaboration helps us to strengthen and continuously improve our product security practices. The following engagements reflect our 2023 contribution to building a strong community of practice:

AdvaMed
Advanced Medical Technology Association

AdvaMed Cybersecurity Working Group

BD participates in the AdvaMed Cybersecurity Working Group, which brings medical device industry professionals together for the purpose of improving cybersecurity in the medical device ecosystem to protect patient safety and sensitive data. In 2023, BD was invited to share insights at the AdvaMed Cybersecurity Summit about implementing the latest FDA cybersecurity requirements. Through the Cybersecurity Working Group, BD also provided comments on emerging cybersecurity developments and multiple industry discussion papers.

http://www.advamed.org/

BIOHACKING VILLAGE

Biohacking Village at DEF CON

The Biohacking Village is a 501(c)3 organization that brings medical, laboratory and pharmaceutical device manufacturers and security researchers together to strengthen medical device security. In 2023, BD sponsored the event as part of our culture of transparency and collaboration. We also submitted a BD research device, comprised of software and a workstation, to the Medical Device Lab for security researchers to perform ethical hacking. Two security researchers reported vulnerabilities to BD. As part of our routine vulnerability disclosure process, we reported the vulnerabilities to the FDA and CISA and shared them with customers through a coordinated vulnerability disclosure. The event also served to strengthen our internal cybersecurity processes.

https://www.villageb.io/

Collaborating to strengthen healthcare cybersecurity

Health Information Sharing and Analysis Center

The Health Information Sharing and Analysis Center (H-ISAC) is a global, non-profit organization driven by its members. It serves as a hub for sharing actionable cybersecurity intelligence and best practices within the healthcare sector. BD regularly shares coordinated vulnerability disclosures with H-ISAC to maximize awareness. In addition, in 2023, BD participated in various working groups and partnered to drive industry best practices into the company's cybersecurity and product security strategies.

https://h-isac.org/

Healthcare Sector Coordinating Council (HSCC) Cybersecurity Working Group

The HSCC Cybersecurity Working Group (CWG) is a coalition of more than 430 industry and government organizations partnering to identify and mitigate cybersecurity threats to health data and research, systems, manufacturing and patient care. BD participates in multiple CWG task groups, including the Medical Technology Cybersecurity Task Group, which recently published the **Medical Device and Health IT Joint Security Plan Version 2.0**. BD also contributed to two resources in 2023: the **Coordinated Healthcare Incident Response Plan (CHIRP)** and **Managing Legacy Technology Security (HIC-MaLTS)**. In addition, BD co-leads the newly established Operational Technology (OT) Manufacturing task group aimed at developing best practices for securing OT manufacturing networks for healthcare manufacturing subsectors. BD also contributed to the **Health Industry Cybersecurity Strategic Plan**, a five-year call-to-action for prioritizing foundational cybersecurity practices across the sector.

https://healthsectorcouncil.org/

International Medical Device Regulators Forum

The International Medical Device Regulators Forum (IMDRF) Cybersecurity Working Group is dedicated to accelerating international medical device regulatory convergence to promote an efficient and effective regulatory model for medical devices to protect public health and safety. BD contributed to two IMDRF documents that were published in 2023: **Principles and Practices for the Cybersecurity of Legacy Medical Devices** and **Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity**.

https://www.imdrf.org/

Medical Device Innovation Consortium

The Medical Device Innovation Consortium (MDIC) seeks to improve health and save lives by accelerating access to medical technologies. In 2023, BD participated in the MDIC cybersecurity steering committee. Through this engagement, we helped increase awareness of the MDIC's cybersecurity benchmarking initiative and contributed to the organization's three-year strategic plan. BD also participated in MDIC's Penetration Testing Best Practices working group.

https://mdic.org/

Collaborating to strengthen healthcare cybersecurity

MedTech Europe

MedTech Europe is the European trade association for the medical technology industry. In 2023, BD participated in the association's Cybersecurity Working Group leadership team. Through this engagement, BD collaborates with fellow cybersecurity leaders, including representatives of the European Union Agency for Cybersecurity (ENISA), to provide recommendations for cybersecurity-related policies. During 2023, the Cybersecurity Working Group focused on European Union (EU) cybersecurity regulations impacting the MedTech industry, including the Network and Information Security Directive (NIS2) and the Cyber Resilience Act.

https://www.medtecheurope.org/

MITRE

MITRE was established to advance national security and apply systems thinking to challenges across government, industry and academia. In 2023, BD participated in MITRE's legacy devices working group and provided feedback on the development of the **Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks** white paper, which the FDA asked MITRE to develop in collaboration with healthcare delivery organizations, medical device manufacturers, federal agencies and other industry stakeholders.

https://mitre.org/

Continuing to advance cybersecurity—together

In healthcare, upholding strong cybersecurity measures is part of honoring the trust our customers, patients and regulators place in BD. As we continue to mature our cybersecurity program and share best practices across the industry, we invite you to partner with us.

To learn more, visit the **BD Cybersecurity Trust Center**.

[1] DBIR: 2023 Data Breach Investigations Report. Verizon. https://www.verizon.com/business/resources/reports/dbir/. Published June 6, 2023. Accessed September 28, 2023.

[2] HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors. U.S. Department of Health and Human Services. https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html. Published December 6, 2023. Accessed December 12, 2023.

[3] HC3: Sector Alert Report: 202308041500. U.S. Health and Human Services. https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf. Published August 4, 2023. Accessed October 22, 2023.

[4] Burgess M. Criminals Have Created Their Own ChatGPT Clones. WIRED. https://www.wired.com/story/chatgpt-scams-fraudgpt-wormgpt-crime/. Published August 7, 2023. Accessed October 22, 2023.

[5] Gartner Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, by analysts Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, Charlie Winckless, published 25 January 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

[6] Collaborating for Resilience in Healthcare: H-ISAC Annual Report 2022. Health Information Sharing and Analysis Center. https://h-isac.org/wp-content/uploads/2023/04/2022_Health-ISAC-Annual-Report-sm.pdf. Published April 3, 2023. Accessed January 20, 2024.

BD

Advancing the
world of health™

BD, Franklin Lakes, NJ, 07417, U.S.
201.847.6800

bd.com