2022 Cybersecurity Annual Report

Cybersecurity by design, in use and through partnership

BD

Advancing the world of health™

Transparency helps protect patient safety and privacy

A message from Rob Suárez, Chief Information Security Officer

Cybersecurity is a discipline at the intersection of people, processes and technology. In healthcare, patient care can be interrupted and even compromised when a medical device cannot be used or trusted because of a cyberattack. That means cybersecurity in healthcare involves more than securing systems and data. It includes protecting patient safety and privacy. We are always mindful that there is a patient at the end of everything we do.

Medical device cybersecurity has become more critical than ever as the number of smart, connected devices grows and healthcare expands into more care settings, including patient homes. Ensuring patient privacy in these care settings is critical. At the same time, cybercriminals continue to attack healthcare entities with attempts to extort money, steal intellectual property and cause disruption.

At BD, we are on a journey toward advancing cybersecurity maturity in our products, manufacturing operational technology (OT) and enterprise information technology (IT). We recognize that cybersecurity threats continue to evolve, and the strategies, processes and tools we use must continue to advance. By protecting BD medical devices, safeguarding our manufacturing capabilities and defending the company's IT infrastructure, we are helping to maintain a thriving and resilient healthcare system.

"In healthcare, cybersecurity involves more than protecting systems and data."

The state of healthcare cybersecurity

The threat landscape in healthcare is expanding and increasing in complexity. Threat actors operate from various motivations, from stealing intellectual property and patient data for financial gain to foreign espionage. To protect patient safety and privacy, healthcare delivery organizations, medical device manufacturers and third-party vendors must all be aware of cybersecurity risks. These risks include ransomware attacks, phishing attacks, insider threats and software vulnerabilities.

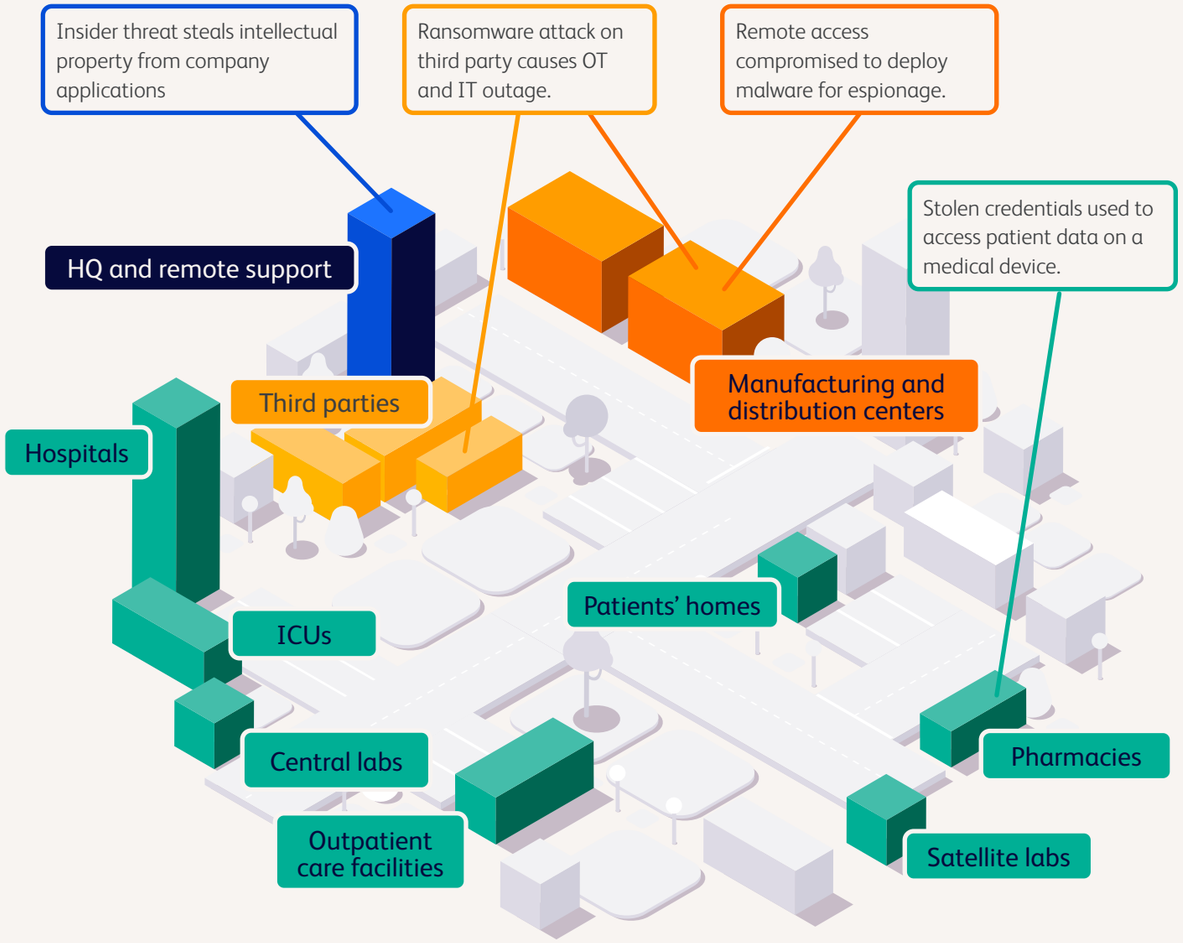
Hospitals, labs, pharmacies—and even patients' homes where software-enabled medical devices are used—must be on guard for these types of threats. To increase awareness, medical device manufacturers, healthcare providers, regulators, security researchers and government agencies must work together to protect patients by sharing leading practices and actionable threat intelligence.

Threat actor motivations:

- Foreign espionage
- Intellectual property
- Patient data
- Financial gain

Key risks include:

- Ransomware attacks
- Insider threats
- Medical device software vulnerabilities
- Third-party software vulnerabilities
- Human error
- Phishing attacks



Cybersecurity trends

Over the last year, three cybersecurity trends have continued to have a significant impact on the healthcare industry:

1. Ransomware attacks remain a specific concern for healthcare.

In 2022, the FBI revealed that it successfully thwarted a planned attack against Boston Children's Hospital in 2021[1]. Attacks like this are a regular occurrence in healthcare. During the first half of the year, 347 organizations reported healthcare data breaches of 500 or more records to the U.S. Department of Health and Human Services (HHS), showing a slight decrease in breaches compared to the first half of 2021[2]. According to a report by SonicWall, ransomware attacks decreased by 23% overall during the first half of 2022 but increased by 328% in healthcare[3]. Several U.S. government agencies, including HHS, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of the Treasury issued alerts in 2022 specifically calling out ransomware attacks aggressively targeting the healthcare sector[4,5,6]. Notably, the alerts warned of increasingly sophisticated techniques, from leveraging a ransomware-as-a-service (RaaS) model to removing system backups to complicate data restoration efforts and encrypting servers that house electronic health records, diagnostic and imaging data, and internet services[4,5].

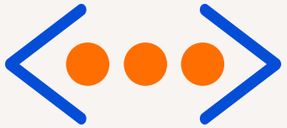
To reduce the risk of ransomware at BD, we continuously monitor network activity in accordance with local laws, manage and reduce the attack surface, and remediate known vulnerabilities. We also maintain strategic resilience measures, including secure backups, and we regularly collaborate with government and industry leaders who share real-time threat intelligence.

2. Phishing remains a common entry point for cybersecurity attacks.

According to a Health Information and Management Systems Society (HIMSS) report, phishing is involved in 57% of the industry's most significant cybersecurity incidents[7]. Phishing attacks are also becoming more sophisticated, with attackers using adversary-in-the-middle (ATM) techniques to bypass multifactor authentication[8,9]. Criminal groups often switch tactics to launch business email compromise (BEC) attacks[10]. These attacks leverage traditional social engineering methods to convince employees to redirect legitimate payments, a crime that may go undetected until the intended payee sends another invoice.

To reduce the risk to BD, we launch training campaigns and each month send global phishing simulation emails to all associates who use a BD email address and an assigned computing device. These simulated attacks mimic real-world strategies used by cybercriminals. Associates who click on the links in these simulated phishing emails receive additional training to reinforce their cyber-smart skills.

Cybersecurity trends



3. Software supply chain attacks emphasize the need for software bill of materials (SBOM) transparency.

Software supply chain attacks increased by 650% during 2021[11]. Gartner® predicts that by 2025 "45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."[12] One example that impacted healthcare over the last year is the Apache Log4j zero-day vulnerability which was publicly disclosed in December 2021. Log4j is an open-source logging framework used in approximately three billion devices that use Java[13], including medical devices, enterprise systems and manufacturing operational technologies. Due to the prolific use of Log4j, the U.S. Food and Drug Administration (FDA) and HHS issued alerts in late 2021 and early 2022 warning about the potential for widespread exploitation[14, 15].

To bolster incident and vulnerability management, the industry is moving toward greater SBOM visibility. The FDA pointed out this need in the agency's updated premarket draft cybersecurity guidance, **Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions**, which was released in April 2022. Having a complete inventory of all software components contained in a medical device, including software developed by the manufacturer and software components developed by third parties—whether purchased off the shelf, licensed or open-source—allows healthcare providers to more quickly and efficiently determine whether they are impacted any time a new vulnerability is disclosed. BD issues Product Security White Papers for each software-enabled product. These documents include a Manufacturer Disclosure Statement for Medical Device Security (MDS2). BD will begin utilizing machine-readable SBOMs in our processes in 2023. We also receive detailed SBOMs from our third-party software component providers, which allows us to more quickly determine which BD systems and products are potentially impacted by emerging vulnerabilities and which are not. This allows us to focus risk mitigation efforts where they are needed most.

With this maturity, assessing BD products and enterprise systems for potential impact will take minutes instead of days. This increase in efficiency matters because cybercriminals scan for vulnerable attack surfaces within minutes when new vulnerabilities are announced[16].

Cyberattacks and patient care

We have known for years that cyberattacks can impact patient care. In 2017, the WannaCry ransomware attacks crippled the United Kingdom's National Health Service (NHS), which led to the cancellation of 19,000 appointments and cost an estimated £92 million[17, 18]. Since that time, numerous cyberattacks have reportedly impacted patient care and outcomes, including attacks that have disrupted emergency transportation systems, disabled patient monitoring alerts and rendered electronic medical records inaccessible.

The CyberMed Summit is a 501(c)(3) organization founded by Dr. Christian Dameff, Medical Director of Cybersecurity at the University of California San Diego, and Dr. Jeff Tully, anesthesiologist and security researcher at the University of California San Diego. The CyberMed Summit seeks to improve patient safety through cybersecurity and builds clinical cyberattack scenarios into its annual conferences.

"These are the types of scenarios we plan for when we conduct clinical cyber simulations during our annual CyberMed Summit," said Dr. Dameff. "Our mission is creating an inclusive, educational and collaborative summit to improve patient safety through cybersecurity. At each CyberMed Summit, we conduct a clinical simulation to demonstrate that cybersecurity can absolutely impact patient care and outcomes."

In 2021, the U.S. Centers for Disease Control (CDC) published research demonstrating the connection between hospital strain and excess deaths during the COVID-19 pandemic. Researchers concluded that when intensive care units reach 75% capacity, surrounding communities experience 12,000 excess deaths in the following two weeks. When hospitals reach 100% capacity, excess deaths skyrocket to 80,000 during the subsequent two-week period[19]. In a report titled "*Provide Medical Care* is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm," CISA concluded that the same type of strain could be caused by cyberattacks, especially in rural areas where there are fewer hospitals to absorb patient overflow[20].

"Any disruption in device availability or integrity can have direct impacts on patient care," said Beau Woods, a Cyber Safety Innovation Fellow with the Atlantic Council and co-founder of I Am The Cavalry, a group of global cybersecurity volunteers with expertise across technology, law and public policy. "When healthcare providers are unable to use or rely on medical devices due to a cyberattack or cyber-related outage, we know patient care and safety can be compromised. While we've yet to see deaths legally and definitively attributed to cybersecurity attacks, we know that potential is there any time life-saving technologies are disrupted by accidents or adversaries. That is why we must continue to strengthen cybersecurity in healthcare, so no patient has to worry about cyberattacks impacting their medical care, safety or privacy."

Emerging cybersecurity developments

2022 was a year of unprecedented cybersecurity developments.

Governments worldwide are becoming more keenly aware of the impact of cyber risks and have begun to enact more aggressive legislation to increase cybersecurity protections. Examples of recent legislation include the following developments aimed at increasing cyber-preparedness:

Singapore

Cybersecurity Labelling Scheme (CLS)

The Cyber Security Agency of Singapore (CSA) updated its Cybersecurity Labelling Scheme (CLS) in October 2022 to include medical devices. Manufacturers are required to attain the CLS Level 1 label when they register their medical devices with the Health Sciences Authority (HSA). BD anticipates that hospitals will look to procure and install medical devices that are at least CLS Level 2 label compliant. CLS Level 3 and CLS Level 4 are voluntary and include independent, third-party assessments.

European Union

EU Cyber Resilience Act

The European Commission proposed the EU Cyber Resilience Act (CRA) in September 2022. This new legislation will introduce mandatory cybersecurity requirements for products with digital elements. It is expected to create requirements for vulnerability management and disclosure, technical documentation and conformity assessment. Non-compliance will result in significant fines of up to 15 million EUR or up to 2.5% of a company's total worldwide annual turnover.

Brazil

Resolution of the Collegiate Board of Directors RDC 657/2022 and RDC 185/2001

Brazil's Health Regulatory Agency, Anvisa, published its Resolution of the Collegiate Board of Directors RDC 657/2022 in March 2022, which provides for the regularization of Software as a Medical Device (SaMD). The agency also announced significant updates to RDC 185/2001 in September 2022. The changes, which will take effect in March 2023, are aimed at strengthening the country's medical device registration regulations.

United States

The Protecting and Transforming Cyber Health Care (PATCH) Act

The PATCH Act was introduced in April 2022. If passed, this legislation would expand on medical device manufacturing regulations, requiring manufacturers to design, develop and maintain updates and patches throughout the life cycle of their devices. Manufacturers would also have to create a thorough plan for addressing post-market cybersecurity vulnerabilities in a timely manner and create a software bill of materials (SBOM) for each product and its components.

Emerging cybersecurity developments

Examples of recent cybersecurity reporting developments include:

United States

The Cyber Incident Reporting for Critical Infrastructure Act

U.S. President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law in March 2022, requiring critical infrastructure entities to report significant cybersecurity incidents to CISA within 72 hours and report ransomware payments to CISA within 24 hours. The Act requires CISA to define what constitutes a covered entity and what types of cybersecurity incidents are deemed significant and therefore trigger the reporting requirements. CISA has 24 months to create a proposed rule and 18 months after that to create a final rule.

United States

Proposed Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure Rules

The U.S. Securities and Exchange Commission (SEC) unveiled proposed cybersecurity disclosure rules in March 2022 that will potentially create more stringent reporting requirements for public companies. If adopted in their current form, the rules will require public companies to make prescribed cybersecurity disclosures, including:

- Mandatory disclosure of material cybersecurity incidents via Form 8-K, within four business days of a company determining that a cybersecurity incident is material in nature.
- Mandatory disclosure of material changes, additions or updates to previously disclosed material cybersecurity incidents (or immaterial cybersecurity incidents not previously disclosed that become material in the aggregate) in the company's Form 10-Q or Form 10-K for the period in which the event occurred.
- Mandatory, ongoing disclosures on companies' governance, risk management and strategy with respect to cybersecurity risks, including board cybersecurity expertise and board oversight of cybersecurity risks.

India

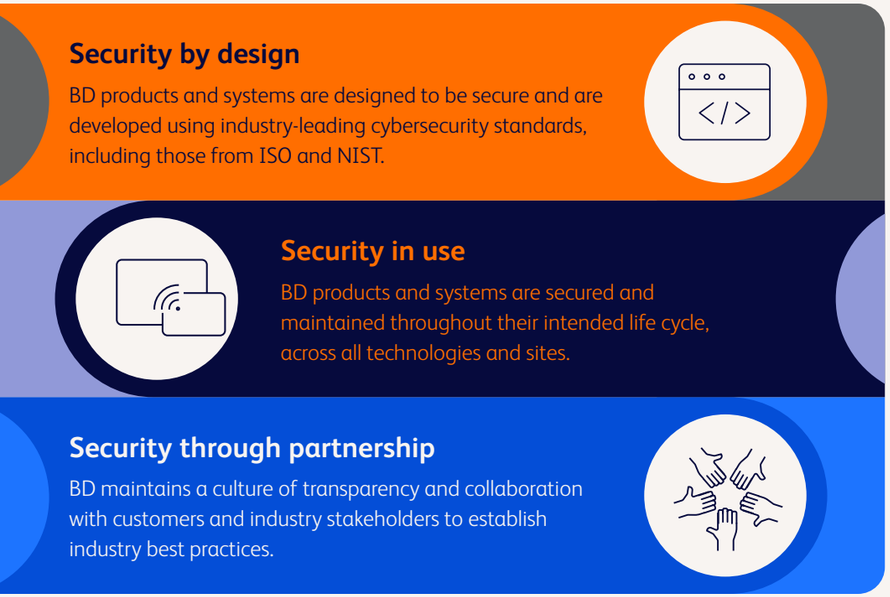
Update to Section 70B of the Information Technology (IT) Act, 2000

In April 2022, the Indian government issued an addendum to section 70B of the Information Technology (IT) Act, 2000, requiring organizations to report cybersecurity incidents to India's Computer Emergency Response Team (CERT-In) within six hours of discovering them. Examples of qualifying incidents include data breaches or leaks, targeted scanning or probing of critical systems or networks, unauthorized access to IT systems or data, and denial of service attacks. This change was entered into force in June 2022[21]. Prior to rule No. 20(3)/2022-CERT-In, India required organizations to notify CERT-In "as soon as possible" following a cybersecurity incident[22].

Cybersecurity at BD

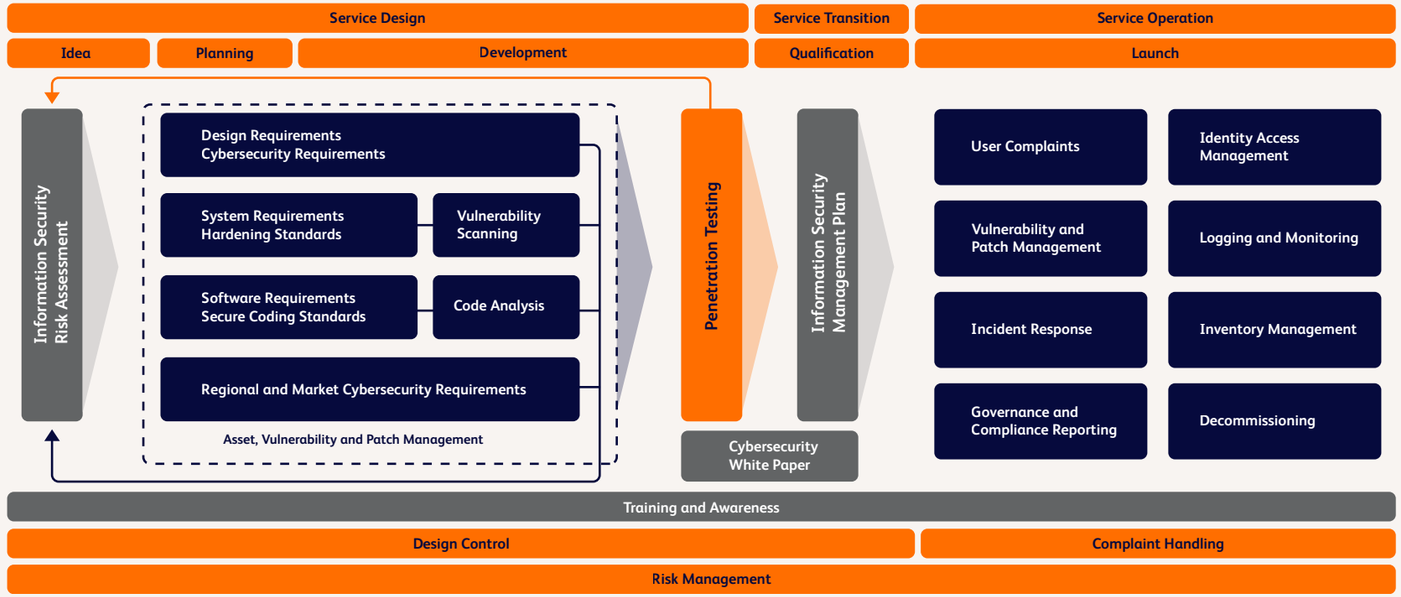
Methodology

Our commitment to cybersecurity includes the protection and resilience of our products, manufacturing and IT. We strive to meet high security standards so our customers can focus on what matters most: caring for patients. We base our strategic approach to cybersecurity on three guiding principles:



BD Cybersecurity Framework

Our Secure Software Development Lifecycle (SSDLC) follows the BD Cybersecurity Framework, which serves as a blueprint for managing cybersecurity risk across BD products, manufacturing operational technology and information technology. The framework incorporates design requirements, including cybersecurity risk assessment, penetration testing, code analysis, system hardening and continuous vulnerability management. It is aligned to multiple industry standards and work products, including the International Organization for Standardization (ISO) 27001 standards, 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, Underwriters Laboratories (UL) 2900 Standard for Software Cybersecurity for Network-Connectable Products and the standards of the International Society of Automation (ISA) 62443.



Cybersecurity preparedness

Just as communities prepare for natural disasters, organizations must prioritize cyber preparedness to prevent and recover from cybersecurity attacks. To enable resilience, it is crucial to identify, assess and mitigate cybersecurity risks. BD operates a 24/7 global cybersecurity operations center (CSOC) and also has dedicated support from regional CSOCs that are responsible for:

Cybersecurity monitoring

The CSOC is responsible for monitoring the corporate network for any unusual events, vetting data to identify security breaches and providing information and support to incident management during an incident. BD proactively monitors for suspicious activity, including phishing attacks, malware and ransomware attacks, insider threats and human error. In 2022, our global CSOC blocked an average of 114 million intrusion attempts per month.

Threat hunting and threat intelligence

The CSOC compiles internal and external threat data to enhance vulnerability knowledge and our understanding of how BD systems may be impacted. This includes insight regarding active campaigns and known threat actor activity. Additionally, the CSOC collaborates with government and industry leaders for threat intelligence, including the Domestic Security Alliance Council, a strategic alliance that includes the U.S. Federal Bureau of Investigation (FBI), U.S. Department of Homeland Security and private industry, and the U.S. FBI InfraGard, a partnership between the FBI and the private sector to protect critical infrastructure.

Incident management

The CSOC helps maintain the confidentiality, integrity and availability of BD systems and data by preparing for and minimizing cybersecurity incident-based losses, theft of information and/or disruption of services that could result in severe loss of information assets, revenue, public confidence, reputation or market share. BD processes and procedures are based on and reference the NIST Special Publication (SP) 800-61 concepts to immediately detect and respond to security incidents. Guidance from data protection regulators is also incorporated during data breach management. Additionally, we follow the Incident Command System (ICS) which explains the relationship with the National Incident Management System (NIMS) and the roles of Emergency Management, as guided by FEMA. Our Incident Vulnerability Management Process is modeled after the NIMS process and includes:

A **Golden hour –** Task Force coordination and engagement; determine initial severity rating

B **Assess and contain –** Validate the vulnerability or incident; identify root cause, scope, impact and short-term workaround/mitigation

C **Remediate –** Define remediation and closure requirements

D **Closure –** Communicate to internal and external stakeholders, where applicable

E **Postmortem –** Review technical impact and communication/coordination lessons learned

Insider threat monitoring and detection

The CSOC identifies BD sensitive data through data tagging and sensitivity labels and focuses on preventing data loss using insider risk management policies and monitoring tools designed to prevent unintentional sharing of intellectual property. BD monitors for critical words and activities, and alerts are triggered if high-risk data leaves the BD environment. Data is monitored for rule disruption on the company's endpoints, network and cloud solutions, which include performing cybersecurity risk assessments.

Proactive and preventive controls

BD continuously applies the following proactive and preventive controls to protect our customers and patients from cyberthreats:

- Monitor network activity in accordance with local laws.
- Manage and reduce the attack surface for potential threat actors.
- Maintain strategic resilience measures, including secure backups.
- Manage geographical segmentation controls where required.
- Perform internal and external security audits and vulnerability assessments.
- Conduct robust risk assessments and penetration testing.
- Perform proactive vulnerability scanning and management.
- Collaborate with government and industry leaders for threat intelligence.
- Evaluate cybersecurity incident response plans and processes.
- Provide ongoing cybersecurity training and awareness among 77,000 BD associates.

Cybersecurity governance

Our approach to cybersecurity governance includes aligning cybersecurity risk management, policy and compliance initiatives with business objectives so that information assets and technologies used in BD products, manufacturing, service, enterprise IT and third-party components are secure, resilient and compliant with applicable regulatory and industry standards.

This includes cybersecurity due diligence for BD mergers, acquisitions and divestitures. BD Information Security policies and procedures are aligned to industry best practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Underwriters Laboratories (UL) 2900-1 Cybersecurity Standard for Medical Devices and FDA pre-market and post-market guidance for cybersecurity in medical devices. BD Information Security policies are reviewed annually by cross-functional stakeholders specializing in information security, integrated supply chain, enterprise IT and quality.

In 2022, BD achieved ISO/IEC 27001:2022 certification at the enterprise level, demonstrating that our Information Security Management System (ISMS) conforms to internationally recognized cybersecurity standards. Additional cybersecurity 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) security rule. 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 multiple BD medical devices through a rigorous program of analysis. For more information about these certifications and attestations, visit the **BD Cybersecurity Trust Center**.

Cybersecurity risks and their potential impact on BD and its customers and patients are reviewed by the company's central, regional and business teams. Information security provides guidance for identifying, prioritizing and mitigating such risks. Cybersecurity risks are also integrated into our approach to enterprise risk management. Timely, impactful cybersecurity information, including cybersecurity metrics, threat briefings and significant cybersecurity risks are communicated to the Executive Leadership team and the Board of Directors through the Audit Committee and the Quality and Regulatory Committee, as well as ad-hoc communications.

In addition, BD provides cybersecurity training for the Board of Directors and the Executive Leadership team. This includes annual scenario-based cybersecurity training for providing effective oversight in the event of a significant cybersecurity incident. It also includes targeted cybersecurity training opportunities such as the National Association of Corporate Directors (NACD) Cyber-risk Oversight Certificate program, which is designed to enhance participants' understanding of the cybersecurity threat landscape, cyber-risk oversight responsibilities and organizational preparedness for cybersecurity crises.

We also provide annual cybersecurity and data protection awareness training for our 77,000 associates, comprised of online cybersecurity training modules; in-person and virtual cybersecurity bootcamp classes; contextual phishing simulation exercises; mock incident response exercises; and intranet resources aimed at enhancing associates' ongoing cyber-awareness.

For more information about our ISO/IEC 27001:2022 certification, read **BD Achieves ISO Certification for its Enterprise-Level Information Security Management System**.

Collaborating to strengthen cybersecurity in healthcare

In addition to taking steps to protect BD, our customers and patients from cybersecurity threats and risks, we also seek to contribute to and learn from the broader community. BD collaborates with customers, government agencies, cybersecurity working groups, security researchers and fellow medical device manufacturers to advance cybersecurity in healthcare. The following engagements reflect our 2022 contribution to building a strong community of practice:

AdvaMed Cybersecurity Working Group

Chaired by BD CISO, Rob Suárez, this working group provided comments on emerging cybersecurity developments, including the FDA's updated premarket draft cybersecurity guidance, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, and the PATCH Act. The working group also provided comments on multiple industry discussion papers, including two International Medical Device Regulators Forum (IMDRF) draft documents: Principles and Practices for the Cybersecurity of Legacy Medical Devices and Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity.

advamed.org

Biohacking Village at DEF CON

The Biohacking Village (BHV) is a 501(c)3 organization that brings medical, laboratory and pharmaceutical device manufacturers and security researchers together to strengthen medical device security. In 2022, we sponsored the event as part of our commitment to transparency and collaboration. We also submitted a medical device for security researchers to perform ethical hacking. They attempted to break into the device just as threat actors would, but for the purpose of identifying previously unknown vulnerabilities in order to safeguard the device from future cyberattacks.

The device was the BD SiteRite™ 9 Ultrasound System, a BD Medical Delivery Solutions vascular access device that provides real-time ultrasound imaging to help visualize blood vessels, needle trajectory and final tip location. At the time, the BD SiteRite™ 9 was not yet commercially available. It was designed using the BD Cybersecurity Framework. Bringing this device to the Biohacking Village allowed us to augment our own penetration testing and further validate the device's cybersecurity posture. While there was significant engagement and interest in the product, security researchers did not identify any new vulnerabilities.

villageb.io

CISA Cyber Storm VIII

Every two years, CISA hosts a national Cyber Storm exercise to bring public and private-sector entities together to simulate how they would respond to incidents impacting the nation's critical infrastructure. In 2022, BD Information Security partnered with CISA to plan the event, which unfolded over three days of live exercise play. The scenario included multiple simulated cyberattacks impacting the healthcare sector and other industries across critical infrastructure. More than 2,000 individuals across federal, state and local governments, the private sector and international organizations participated.

cisa.gov/cyber-storm-securing-cyber-space

Collaborating to strengthen cybersecurity in healthcare

HSCC Cybersecurity Working Groups

BD participates in multiple Healthcare and Public Health Sector Coordinating Council (HSCC) cybersecurity task groups. In 2022, we contributed to several industry work products published by the organization over the last year, including:

- **The Operational Continuity Cyber Incident (OCCI) Checklist,** which was published in April 2022 to help security operations and executive management respond to and recover from an extended enterprise outage in the event of a significant cyberattack.
- **The MedTech Vulnerability Communications Toolkit,** which was published in April 2022 to help medical device manufacturers create consistent cybersecurity vulnerability communications related to their products or services.
- **The Model Contract-Language for MedTech Cybersecurity (MC2),** which was published in April 2022 to facilitate alignment between medical device manufacturers and healthcare delivery organizations for cybersecurity and device management.

healthsectorcouncil.org

International Medical Device Regulators Forum

In 2022, BD helped draft two international guidance documents in collaboration with the International Medical Device Regulators Forum (IMDRF), regulators, healthcare providers and medical device manufacturers from around the globe. One is a document about software bill of materials (SBOM) transparency, which will aid healthcare providers and medical device manufacturers in addressing risks associated with vulnerable software components. The other focuses on legacy medical devices and how MedTech companies can help healthcare providers prepare for device end of support. Both documents are expected to be published in 2023.

imdrf.org

Medical Device Innovation Consortium

BD participated in several Medical Device Innovation Consortium (MDIC) initiatives in 2022. BD CISO, Rob Suárez, chaired the MDIC Cybersecurity Program Steering Committee, which launched the **Medical Device Cybersecurity Maturity Survey** in collaboration with the HSCC. The MDIC established a benchmark measurement of the medical device industry's cybersecurity maturity by aggregating participating organizations' survey results. This initiative helps MedTech companies track their progress toward advancing cybersecurity maturity and make improvements over time. BD also contributed to the organization's penetration testing white paper to help fellow medical device manufacturers pen test their devices.

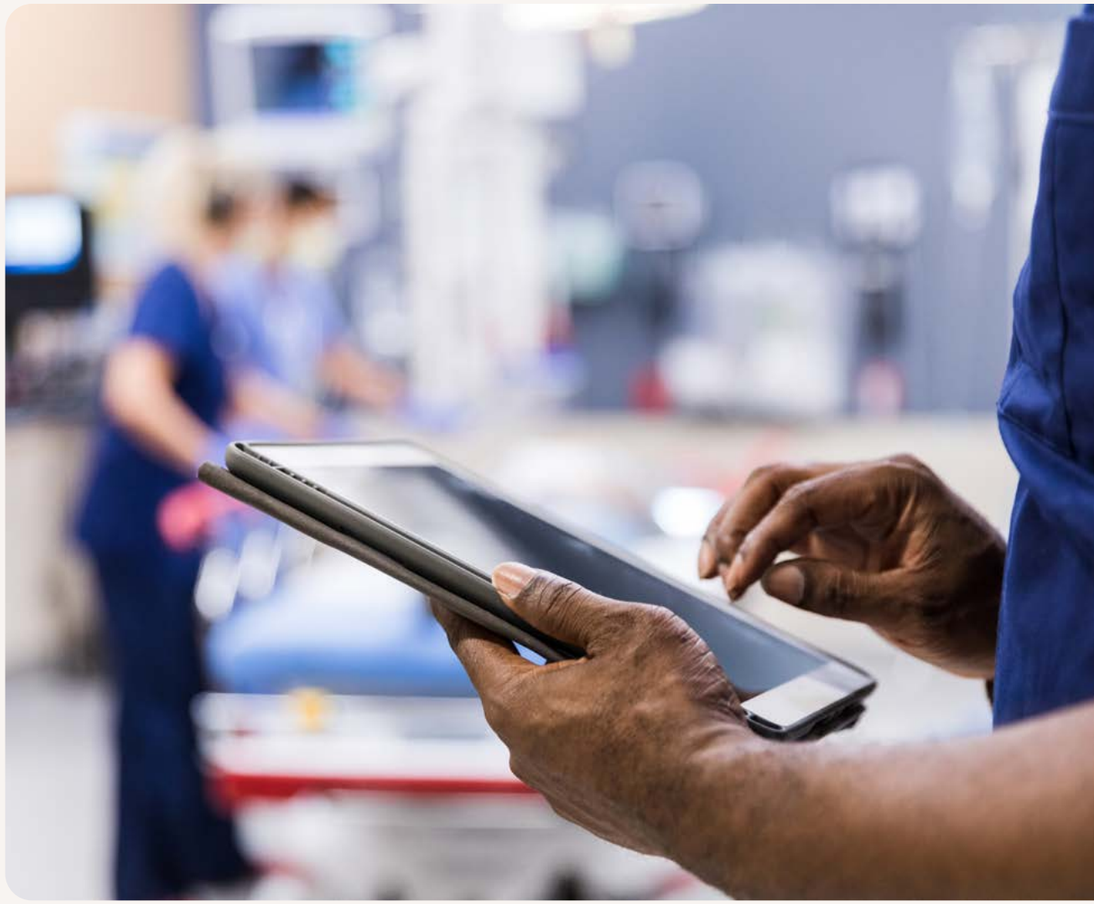
mdic.org

The real-world impact of collaboration

Cybersecurity threats in the bioeconomy have impacted patient safety and privacy. These events validate the reason for MedTech companies to work collaboratively with security researchers to increase understanding of how devices and environments could be breached. From 2020 to the present, we have seen and experienced unprecedented increases in cyberattacks on the healthcare industry, combined with the devastating impact of healthcare worker fatigue. It is essential that we take every opportunity to learn from one another, share our findings and use that information to make medical device technology more secure.

Nina Alli, MSc, MS
Biohacking Village, Executive Director

Securing the medical device ecosystem



Maintaining devices over their intended life cycle is essential to protecting them from emerging cyber risks and threats. Healthcare providers are encouraged to set devices up according to manufacturer guidelines, keep operating systems current and patch known vulnerabilities in a timely manner. In addition, using a device longer than its intended life cycle can have unintended consequences. End-of-life (EoL) and end-of-support (EoS) devices may no longer receive critical cybersecurity updates.

To help healthcare providers manage risk properly through awareness and guidance, MedTech companies must serve as trusted advisors. This begins on day one and continues throughout the intended life cycle of the device.

Product security communications

Regulatory agencies around the world, including the FDA, lay out clear expectations that medical device manufacturers will provide cybersecurity documentation to help healthcare providers apply cybersecurity controls that are suited to the environment in which the device will be used. To provide this information, BD publishes Product Security White Papers for each of its software-enabled products. These white papers, which are available to customers through the **BD Cybersecurity Trust Center**, provide details regarding how BD security and privacy practices have been applied and what customers should know about maintaining security throughout the intended product life cycle.

It is also important for customers to know about new vulnerabilities as they emerge. For more information about our vulnerability disclosure process, turn to **page 14**.

Cybersecurity templates

To accelerate the adoption of strong cybersecurity practices in healthcare, BD makes cybersecurity templates available on the **BD Cybersecurity Trust Center**. These templates can help medical device manufacturers develop product security policies, procedures, incident and vulnerability management plans, and product security white papers.

Coordinated vulnerability disclosure

Responsible vulnerability disclosure is essential to securing the medical device ecosystem. All software-enabled technologies possess cybersecurity risks; cyberattacks can impact even the most mature technology companies. BD has established a program for managing cybersecurity risks over the intended life cycle of our products. This includes a process for responding to vulnerabilities and incidents in a timely and effective manner.

BD is committed to transparency because customers cannot protect patients, devices, systems or data from vulnerabilities they do not know about. We welcome vulnerability reports from customers, security researchers, third-party component vendors and other external groups. When a vulnerability is discovered and validated in a BD product, we follow the **FDA's Postmarket Management of Cybersecurity in Medical Devices** 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 works directly with our third-party partners to determine whether BD products are impacted. In such cases, 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 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 risk properly through awareness and guidance.

Coordinated vulnerability disclosure process

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 and confirm the vulnerability. If confirmed, we follow an Incident Response and Vulnerability Management Plan, which is a strategy BD established to effectively respond to reported cybersecurity issues. Once validated, our incident response team collaborates with various functional teams including Product Security, Research and Development, Quality and Privacy to determine objectives, scope, severity, analysis and the appropriate actions needed to accurately respond to the issue.

Coordinate

BD follows the FDA's **Postmarket Management of Cybersecurity in Medical Devices** guidance to properly communicate confirmed vulnerabilities in BD products in coordination with a Computer Emergency Readiness Team (CERT). We work with CISA to prepare coordinated vulnerability disclosures for our respective websites, and we also voluntarily report the vulnerability to the FDA.

Disclose

Bulletins are published on the **BD Cybersecurity Trust Center** and the **CISA website** in coordinated fashion. For maximum awareness, we also share BD vulnerability disclosures with Information Sharing Analysis Organizations (ISAO) where BD participates, including the **Health Information Sharing and Analysis Center (H-ISAC)** and the **ECRI Institute**.

Investing in cybersecurity

As cyberthreats continue to evolve, organizations must adapt and continuously improve. The following 2023 initiatives exemplify our commitment to making BD products, manufacturing and IT more secure and resilient:

Across the Organization

Extend our cybersecurity community of practice - Advance the organization's cybersecurity maturity by embedding cyber expertise in key functional areas, including IT and R&D.

Launch Cybersecurity Risk Committee (CRC) - The CRC will serve as the management-level governance body for oversight of all cybersecurity risk at BD.

Cybersecurity certifications – Having achieved enterprise-level ISO/IEC 27001:2022 certification in 2022, we plan to pursue additional third-party cybersecurity certifications in 2023, such as the U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC), pending the release of new guidelines.

Product Security

Security by design – Continue to strengthen our product development capabilities to safeguard BD products, automate security scanning and analysis, and drive security considerations early in the design process.

Software bill of materials (SBOM) – Develop machine-readable SBOMs for our software-enabled products, driving automation in vulnerability monitoring and accelerating response and communications for customers.

Secure software development life cycle (SSDLC) – Expand adoption of software code signing and leverage automation to strengthen the cybersecurity of our software supply chain.

Patch management – Drive capability maturity for updateability and patchability for products and develop an end-of-support strategy for legacy products.

Manufacturing Security

Improve Operational Technology (OT) capabilities – Continue to enhance our OT cybersecurity strategy to prioritize ransomware mitigation and continuous cyber risk management across the company's manufacturing sites and distribution centers. This includes increased OT network visibility, segmentation and monitoring to boost incident response capabilities.

IT Security

Implement advanced cybersecurity technologies – Continue implementing a suite of advanced cybersecurity technologies that will increase the company's overall security posture, both in the cloud and on premise, and enhance protection against current and emergent cyberthreats.

Zero Trust architecture – Continue to adopt Zero Trust principles by strengthening and unifying the adoption of single sign-on, conditional access, user behaviors and device health, as well as multifactor and password-less authentication. This approach protects BD and our customers by managing and granting access based on the continuous verification of identities, devices and services.

BD works diligently to help protect the confidentiality, integrity and availability of BD products, manufacturing systems and enterprise IT.

Through these efforts, we are working to improve the resilience of healthcare around the world. We recognize that patients receive medical care at some of the most critical and vulnerable moments in their lives. They trust the safeguards put in place to protect their safety and privacy. In healthcare, upholding strong cybersecurity measures and continuing to advance cybersecurity is part of honoring that trust.

As we continue to move forward as an industry, we invite you to partner with us in this effort. To learn more, visit the **BD Cybersecurity Trust Center**.

1 Tucker E. and Suderman A. Wray: FBI blocked planned cyberattack on children's hospital. AP News. https://apnews.com/article/russia-ukraine-technology-health-middle-east-e4f8e7145e4b4447a331d4b0cc5a5bd3. Published June 1, 2022. Accessed June 6, 2022.

2 1H 2022 Healthcare Data Breach Report. HIPAA Journal. https://www.hipaajournal.com/1h-2022-healthcare-data-breach-report/. Published August 11, 2022. Accessed September 29, 2022.

3 2022 SonicWall Cyber Threat Report. SonicWall. https://www.sonicwall.com/2022-cyber-threat-report/. Published July 26, 2022. Accessed October 4, 2022.

4 Hive Ransomware. U.S. Department of Health & Human Services. https://www.hhs.gov/sites/default/files/hive-ransomware-analyst-note-tlpwhite.pdf. Published April 18, 2022. Accessed October 4, 2022.

5 Alert (AA22-187A): North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/alerts/aa22-187a. Published July 6, 2022. Accessed October 4, 2022.

6 Alert (AA22-223A): #StopRansomware: Zeppelin Ransomware. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/alerts/aa22-223a. Published August 11, 2022. Accessed October 4, 2022.

7 2021 HIMSS Healthcare Cybersecurity Survey. Healthcare Information and Management Systems Society (HIMSS). https://www.himss.org/resources/himss-healthcare-cybersecurity-survey. Published January 28, 2022. Accessed October 5, 2022.

8 Brinkmann M. Officer Phishing Attack circumvents multi-factor authentication. https://www.ghacks.net/2022/07/17/office-phishing-attack-circumvents-multi-factor-authentication/. Published July 17, 2022. Accessed August 19, 2022.

9 From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud. Microsoft. https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/#:~:text=A%20large%2Dscale%20phishing%20campaign,enabled%20multifactor%20authentication%20(MFA). Published July 12, 2022. Accessed August 19, 2022.

10 Business Email Compromise: The $43 Billion Scam. The Federal Bureau of Investigation. https://www.ic3.gov/Media/Y2022/PSA220504. Published May 4, 2022. Accessed June 6, 2022.

11 Check Point 2022 Cyber Security Report. Check Point. https://resources.checkpoint.com/cyber-security-resources/check-point-softwares-2022-security-report. Published January 21, 2022. Accessed October 12, 2022.

12 Gartner Article, 7 Top Trends in Cybersecurity for 2022, April 13, 2022. https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022. 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.

13 Slabodkin G. FDA warns about Log4j cybersecurity vulnerabilities in medical devices. MedTech Dive. https://www.medtechdive.com/news/fda-warns-log4j-cybersecurity-risks-medical-devices/611773/. Published December 20, 2021. Accessed November 9, 2022.

14 Log4J Vulnerabilities and the Health Sector. U.S. Department of Health & Human Services. https://www.hhs.gov/sites/default/files/log4j-vulnerabilities-health-sector.pdf. Published January 20, 2022. Accessed November 9, 2022.

15 Cybersecurity Vulnerability with Apache Log4j. U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#news. Published December 17, 2021. Accessed November 9, 2022.

16 Dinu C. Attackers Conduct a Vulnerability Scan Once Every Hour, New Research Reveals. https://heimdalsecurity.com/blog/attackers-conduct-a-vulnerability-scan-once-every-hour/. Published May 20, 2021. Accessed October 12, 2022.

17 Palmer D. This is how much the WannaCry ransomware attack cost the NHS. ZD Net. https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/. Published October 12, 2018. Accessed October 24, 2022.

18 Field M. WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled. The Telegraph. https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/. Published October 11, 2022. Accessed October 24, 2022.

19 French G, Hulse M, Nguyen D, et al. Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic — United States, July 2020–July 2021. MMWR Morb Mortal Wkly Rep 2021;70:1613–1616. DOI: http://dx.doi.org/10.15585/mmwr.mm7046a5.

20 *Provide Medical Care* is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf. Published September 2021. Accessed November 8, 2022.

21 Toulas B. India to require cybersecurity incident reporting within six hours. Bleeping Computer. https://www.bleepingcomputer.com/news/security/india-to-require-cybersecurity-incident-reporting-within-six-hours/. Published April 29, 2022. Accessed August 19, 2022.

22 McClelland T., Long B., et al. Inside India's New 6 Hour Cybersecurity Incident Notification Requirement. Law.com. https://www.law.com/legaltechnews/2022/05/23/inside-indias-new-6-hour-cybersecurity-incident-notification-requirement/?slreturn=20220719144318#:~:text=The%20new%20direction%20requires%20that,effective%20on%20June%2027%2C%202022. Published May 23, 2022. Accessed August 19, 2022.

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

bd.com

BD
Advancing the world of health™