BD 2020 Cybersecurity Report

Improving cybersecurity collaboration across the industry

BD

Cybersecurity for our customers and patients

A message from VP and CISO, Rob Suárez

At BD, our Purpose is *advancing the world of health*™. From life-saving medical devices and diagnostics tests, to high-tech instruments and equipment, the products we offer are critical to addressing some of the most challenging global health issues—including the COVID-19 pandemic.

The healthcare industry has experienced an increase in cyberattacks since the pandemic began, with cybercriminals targeting hospitals, critical healthcare institutions, and even research organizations working to develop vaccines. These attacks make it clear that cybersecurity matters more now than ever before. It's about protecting what matters most—patient safety and patient privacy—while maintaining a resilient and thriving healthcare system.

BD customers around the world, and their patients, trust us to integrate cybersecurity into our products and to protect the design, manufacturing, delivery and support of those products. Further, our commitment to cybersecurity goes beyond protecting BD products by design to helping customers securely use our products in their environments.

"It's about protecting what matters most—patient safety and patient privacy—while maintaining a resilient and thriving healthcare system."

I am proud to say that BD is committed to doing what is right as we continue our journey toward advancing cybersecurity in the healthcare industry. That means being transparent and enabling customers to manage potential risks properly through awareness and guidance, building a strong community of practice that facilitates the adoption of emerging best practices, and collaborating with industry regulators, global thought leaders, and security researchers around the world who share our commitment to patient safety and patient privacy.

Methodology

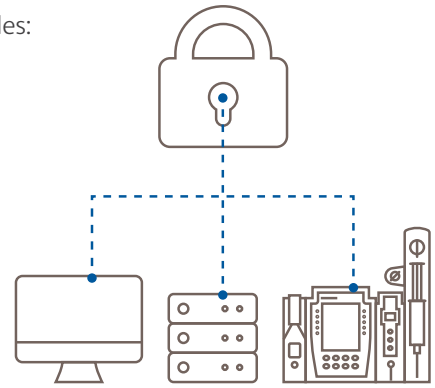
Cybersecurity guiding principles

Our commitment to cybersecurity includes the protection and resilience of our products, manufacturing and IT. We strive to meet high security standards. We also recognize that new security threats emerge daily across the healthcare industry—which is why we believe transparency and collaboration are essential.

Our strategic approach to cybersecurity includes:

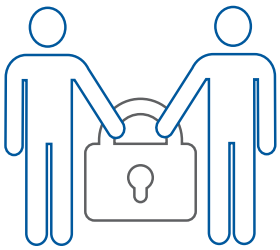
Security by design

BD products and systems are designed to be secure and are developed using industry-leading cybersecurity standards, including those from ISO and NIST.



Security in use

BD products and systems are secured and maintained throughout their intended life cycle, across all technologies and sites.



Security through partnership

BD maintains a culture of transparency and collaboration with customers and industry stakeholders to establish industry best practices.

The current state of healthcare cybersecurity

Cybersecurity is one of the most critical issues impacting the healthcare industry. In 2019, 95 percent of healthcare institutions reported that they were targeted by some form of cyberattack,[1] from attempts at compromising patients' protected health information (PHI) to coordinated efforts to disrupt the healthcare supply chain and clinical workflows at hospitals.

Healthcare data breaches cost an average of $6.45 million, which is 60 percent higher than the global average across all industries.[2] Add to that, the number of connected medical devices has increased by 62 percent in the past 5 years and is expected to continue growing.[1] However, 84 percent of hospitals report operating without a dedicated cybersecurity executive.[3]

Networked medical devices are not created in a vacuum, but rather are an amalgamation of operating systems, hardware and software applications. Without a robust software bill of materials and vulnerability tracking, customers may not know that a device they're using could be vulnerable to attack. The same goes for products that have hit their end-of-life and are no longer being supported by the manufacturer.

In this report, we will share the BD approach to cybersecurity in promoting collaboration across the industry and supporting our customers by addressing both the cybersecurity challenges and trends we see ahead.

COVID-19 and cybersecurity

Despite the global pandemic, the onslaught of attacks did not cease. If anything, the healthcare industry became a bigger target. In April 2020, early in the pandemic, Google recorded an average of 18 million daily malware and phishing emails related to COVID-19 scams.[4] By May of 2020, the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released a joint statement regarding increased cyberattacks against U.S. organizations conducting COVID-19 research and working to develop vaccines, treatments and testing.[5] Amid an increase in ransomware attacks, CISA, the FBI and the Department of Health and Human Services (HSS) issued an additional joint cybersecurity advisory in the fall of 2020, warning U.S. hospitals and healthcare providers about ransomware activity targeting the healthcare and public health sector.[6] In the days that followed, dozens of U.S. hospitals were impacted by Ryuk ransomware, similar to the WannaCry ransomware attacks from 2017.[7]

Improving cybersecurity collaboration across the industry

Teaming up to advance cybersecurity maturity

From industry regulators and healthcare providers to security researchers and medical technology companies, we share the same goals: protecting patient safety and privacy; creating the resilient delivery of healthcare; and accelerating cybersecurity maturity across the healthcare industry.

Over the years, BD has actively sought to quickly align as the industry has made significant advances toward improving cybersecurity. The FDA published final guidance for **Content of Premarket Submissions for Management of Cybersecurity in Medical Devices** in 2014, encouraging medical device manufacturers to address cybersecurity throughout the product life cycle. That guidance is soon to be updated with additional recommendations related to device design, labeling and documentation.[8] Just two years later, in 2016, the FDA published final guidance for **Postmarket Management of Cybersecurity in Medical Devices**, with recommendations for managing and communicating cybersecurity vulnerabilities.

These guidance documents have revolutionized medical device cybersecurity, and what's next is the harmonization of medical device regulations around the world. One organization that's addressing this is the International Medical Device Regulators' Forum (IMDRF), which published **Principles and Practices for Medical Device Cybersecurity** in March 2020. BD was a member of the IMDRF Cybersecurity Working Group, highlighting the need for greater transparency around device end of life (EoL) and end of support (EoS).

In the clinical setting, it is not uncommon to see medical devices in service for 10–15 years,[9] and many are legacy devices that no longer receive regular security updates, putting them at greater risk for cyberattack. Fostering clear communication between medical device manufacturers and healthcare providers around the total product life cycle, including EoL and EoS, equips organizations to better align cybersecurity initiatives with procurement processes in a way that protects patient privacy and patient safety, and reduces the volume of outdated devices on the hospital network.

It's also time to develop a benchmark for cybersecurity maturity, so medical device manufacturers and healthcare providers can identify where they stand in relation to their peers, and where they're headed. A "map" for evaluating cybersecurity maturity already exists in the **Healthcare & Public Health Sector Coordinating Council (HSCC) Medical Device and Health IT Joint Security Plan (JSP)**, which not only outlines specific recommendations for developing, deploying and supporting secure medical devices and health IT products, but also includes Maturity Model Metrics.

The Medical Device Innovation Consortium (MDIC) Cybersecurity Steering Committee, chaired by BD Vice President and Chief Information Security Officer, Rob Suárez, is working to develop a maturity model benchmark based on the JSP Maturity Model Metrics—which include organization structure and governance, risk management, design control and complaint handling—while also drawing on best practices from the Capability Maturity Model Index (CMMI). This benchmark will help medical device manufacturers and healthcare information technology companies track and measure their own progress and maturity against the JSP, while also benchmarking cybersecurity across the industry, adding much needed visibility to the industry-wide progress.

Cybersecurity maturity

What do these advances mean for healthcare providers and patients?

The industry is maturing, and yet it can still be difficult for healthcare providers to know which initiatives to look for and prioritize when entrusting a medical device manufacturer with patient safety and patient privacy. The following best practices have helped BD advance cybersecurity maturity within our own organization:

Threat modeling

Threat modeling is the practice of identifying and prioritizing potential cybersecurity threats and mitigations in order to protect something of value—such as confidential data or intellectual property. In threat modeling, we ask ourselves four basic questions:

- What are we building?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

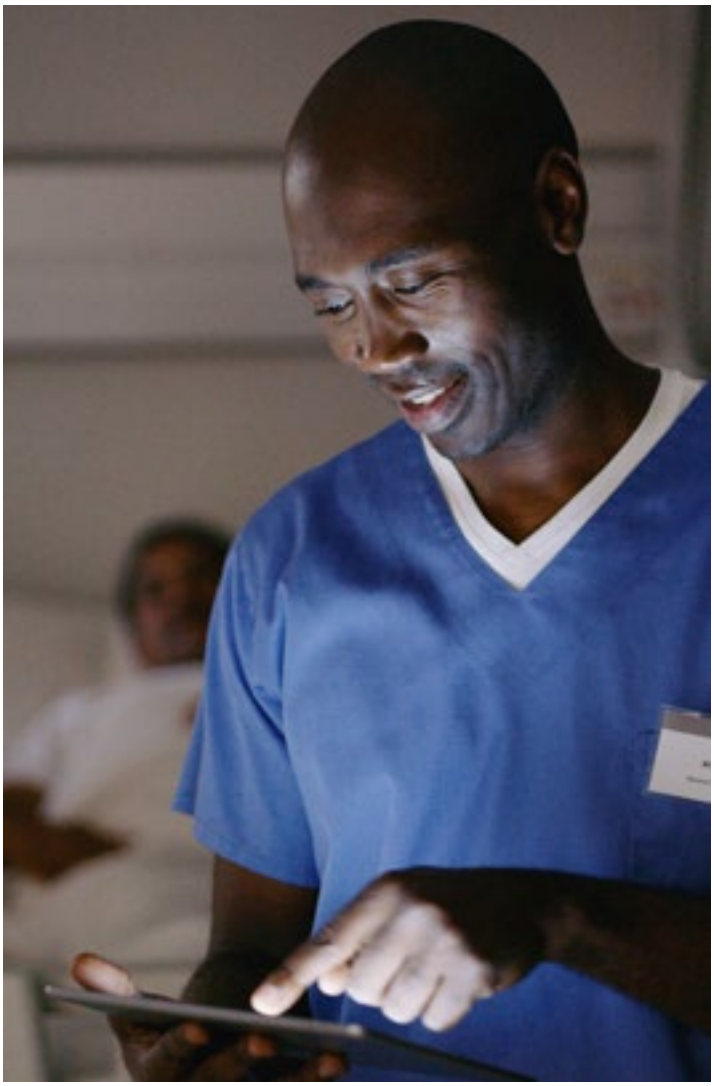
While we design our products to be secure, threat modeling helps us uncover and examine potential risks during the design process and beyond. What we learn from this process helps us improve product security and also communicate mitigations and security best practices to our customers.

Software bill of materials (SBOM)

Medical device technologies often include third-party components. Challenges arise when those components have vulnerabilities that need to be patched. At BD, we strive for transparency, maintaining Product Security White Papers for all software-enabled products—including any third-party component within the BD device. The purpose of these documents is to provide details regarding how BD security and privacy practices have been applied and what our customers should know about maintaining security throughout the entire product life cycle. Each white paper also includes a Manufacturer Disclosure Statement for Medical Device Security (MDS2). Customers and prospective customers can request Product Security White Papers through the **BD Cybersecurity Trust Center**.

Third-party validation

Our cybersecurity programs and policies for products have been evaluated by the Underwriters Laboratories Cybersecurity Assurance Program (UL CAP), which uses standardized, testable criteria to enhance security controls and reduce cybersecurity vulnerabilities. Two BD products, the BD FACSLyric™ Flow Cytometer and the BD Synapsys™ Microbiology Informatics Solution were among the first medical devices to earn UL CAP certification, with additional evaluations underway.



BD also maintains a SOC2+ program for multiple BD products and systems that collect and process patient health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA). These annual audits address the trust principles for security and, for our cloud-based products, availability. SOC2+ 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 and SOC2+ reports are available to customers upon request via the **BD Cybersecurity Trust Center**.

Cyber storm exercises

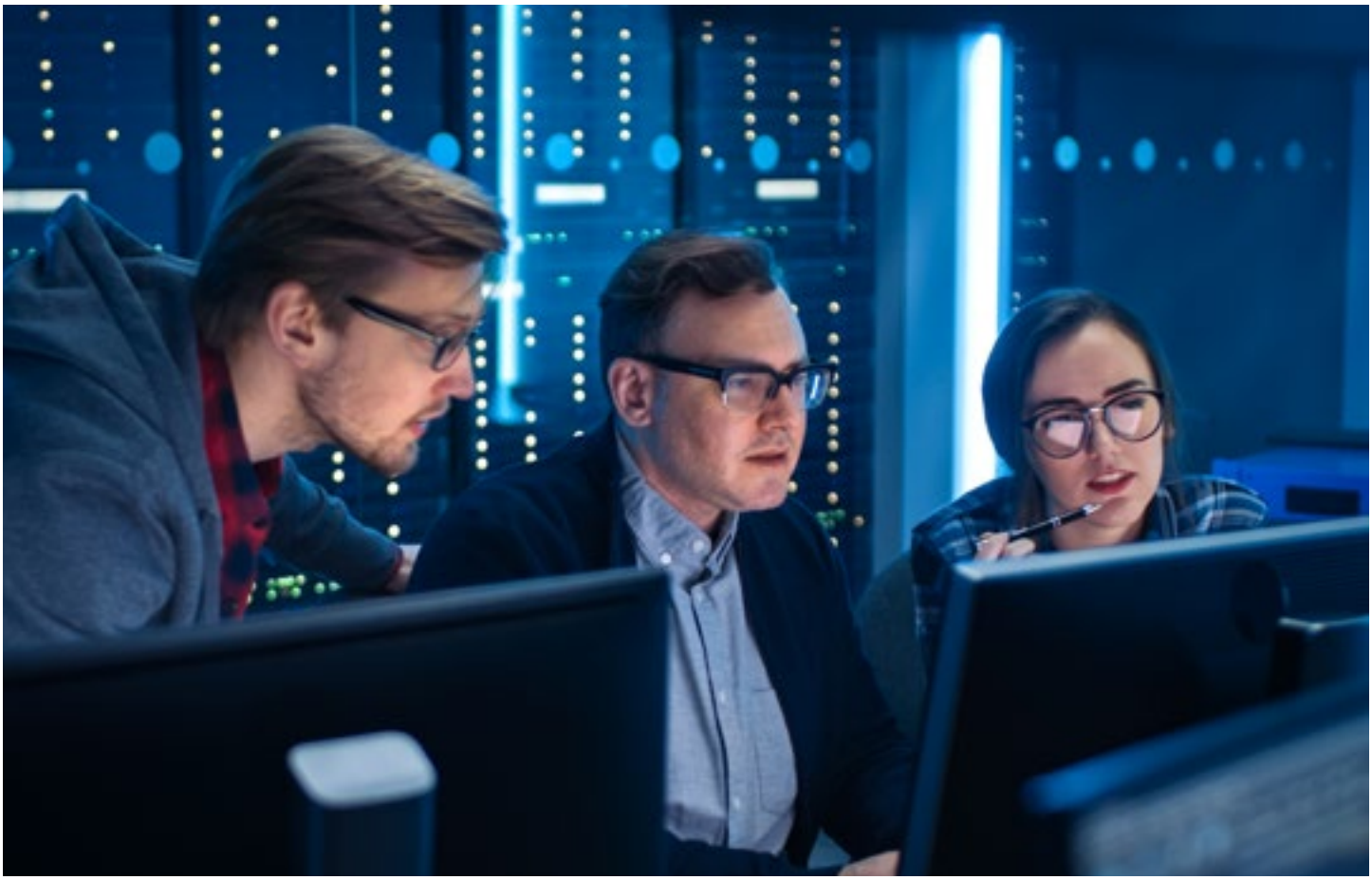
Ninety percent of cyber incident response is preparation. That is why BD participates in cyber storms and tabletop exercises to practice responding to simulated cyber emergencies. In August 2020, the **US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)** facilitated a national cyber storm exercise, bringing public- and private-sector entities together to simulate how they would respond to a cyber crisis impacting the nation's critical infrastructure. More than a dozen cybersecurity professionals from BD participated in **Cyber Storm 2020**, which was designed to test the organization's cybersecurity preparedness and practice incident response and information sharing in a realistic scenario. Additionally, BD partners with CISA to improve internal processes and executive leadership preparedness trainings.

Threat intelligence

Across the healthcare industry, new cybersecurity threats emerge daily. Since you cannot protect what you do not know, it is essential for healthcare providers to understand the threat landscape and have access to reliable information as new vulnerabilities emerge. At BD, we leverage industry, government and law enforcement partnerships in conjunction with commercial threat intelligence solutions to monitor for vulnerabilities and threat activity related to our products and our internal systems.

Vulnerability and incident management

Once a potential vulnerability is discovered or an incident is reported to BD, we work to identify any vulnerable enterprise systems and products, test them, develop and validate compensating controls and/or security updates (as needed), and disclose our findings publicly, equipping customers with the information they need to manage potential risks properly. To learn more about the measures BD takes to drive toward 30-day communication and 60-day remediations for all vulnerabilities and incidents, visit the **BD Cybersecurity Trust Center**.



Looking to advance your organization's cybersecurity maturity?

In addition to our Incident and Vulnerability Management Plan, BD offers an array of cybersecurity templates available for download on the **BD Cybersecurity Trust Center**.

Vulnerability disclosure

Building trust through Coordinated Vulnerability Disclosure

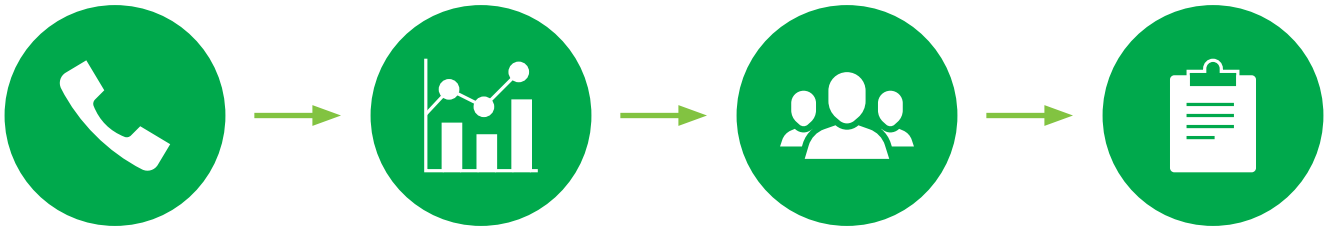
The FDA has established the expectation that all medical device manufacturers communicate *easily exploitable vulnerabilities*, also known as "uncontrolled risks," to customers within 30 days and remediate those vulnerabilities within 60 days.

At BD, we are committed to upholding the same rigorous standard for vulnerabilities that are *difficult to exploit*, otherwise known as "controlled risks." We believe this level of transparency is essential to enabling our customers to manage potential risks properly. All BD product security bulletins and notifications are posted to the **BD Cybersecurity Trust Center**.

We share this information even when a potential vulnerability exists in third-party software. This transparency is standard best practice. Third-party vulnerabilities will continue to exist as new technologies emerge, and BD actively monitors for them so our customers can prioritize patching as needed. Medical device manufacturers have an essential role in protecting the infrastructure of healthcare across the world, and we need to be proactive and share information about the latest emerging threats, new vulnerabilities in our technologies, and what our stakeholders can do to protect themselves. We firmly believe transparency cultivates trust, and we encourage all medical device manufacturers to adopt the same approach.

Likewise, in the spirit of collaboration, BD also voluntarily reports coordinated vulnerability disclosures to the US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), the FDA and the Health Information Sharing and Analysis Center (H-ISAC). We do this to help strengthen cybersecurity across the industry.

Process overview



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.

Analysis

BD partners with the vulnerability reporter to investigate and confirm the validity of the vulnerability.

Coordination

If confirmed, in coordination with existing policies and procedures, BD will perform a cybersecurity risk assessment, clinical risk assessment, and if applicable, conduct validation and remediation planning while concurrently notifying and reporting to various stakeholders.

Disclosure

Through coordinated vulnerability disclosure, BD publishes the contents of the notification on the **BD Cybersecurity Trust Center** and voluntarily reports the vulnerability to Information Sharing and Analysis Organizations (ISAOs) where BD participates, including the Cybersecurity and Infrastructure Security Agency (CISA) and the Health Information Sharing and Analysis Center (H-ISAC).

Report a potential vulnerability or concern

We encourage BD customers and security researchers to engage in a dialogue through proactive reporting. To report a potential product-related security issue (such as an incident, data breach or vulnerability), please complete a **Cybersecurity Issue Report Form** online or email **cybersecurity@bd.com**.

Future trends

What comes next?

As an industry, we've made significant progress in driving collaboration and improving medical device cybersecurity. However, the world continues to change, especially in the face of the COVID-19 pandemic. What can healthcare providers and their patients expect in the year to come? Here's a glimpse at the trends we anticipate:

1. **Continued, systemic cyberattacks targeting the healthcare industry at large.** COVID-19 inspired an unprecedented increase in cyberattacks targeting the healthcare industry at large, from the World Health Organization to pharmaceutical companies working toward a coronavirus vaccine.[10] While the spike was undeniably connected to the virus, it is unlikely that cybercriminals will scale back their attempts in the coming months.
2. **Ongoing challenges related to remote work.** When the pandemic began, millions of healthcare organizations around the world went remote, almost overnight. From virtual telehealth appointments to using medical technology to monitor patients at home, many of these changes will continue long after the pandemic. As a result, healthcare providers and medical device manufacturers must work together to anticipate and effectively manage potential risks across an increasing number of environments.
3. **More sophisticated social engineering attacks.** From phishing attempts to spoofing, social engineering attacks are common because they've been effective. As we look to the future, we can anticipate even more sophisticated social engineering attempts as cybercriminals track what works and find new ways to gain the trust of unsuspecting victims.
4. **An increase in ransomware attacks against healthcare providers.** From WannaCry to Ryuk, ransomware attacks have increased in recent years and continue to be used by threat actors seeking financial gain.[11] Healthcare providers have already begun to examine vendors' cybersecurity maturity more closely, including disaster recovery plans for cloud-based software solutions. As additional ransomware attacks emerge, customers will also increasingly look to vendor partners for support recovering data following these types of targeted attacks against hospital networks.
5. **Expanded adoption of Zero Trust principles.** Improving the resilience of healthcare will need to include an important paradigm shift: adopting Zero Trust principles. Instead of trusting devices inside the network, this approach means trusting no one by default and operating as though the network has already been compromised. Instead of relying primarily on strong passwords and virtual private networks (VPNs), we need to incorporate additional criteria to authenticate and authorize access—such as location, user behaviors and device health—to strengthen our approach and take cybersecurity to the next level.
6. **Additional privacy legislation proposals and new laws.** Globally, we will continue to see regional privacy laws emerge, similar to the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This means that healthcare providers and medical device manufacturers can expect more nuanced and complex privacy regulations in the year ahead.
7. **Increased collaboration within the industry.** Collaboration makes us stronger. While we've made significant progress as an industry, in collaborating with customers, industry regulators, and security researchers, we anticipate increased proactive collaboration between medical device manufacturers in the coming year. Collaboration helps us amplify emerging threats, accelerate knowledge sharing about third-party vulnerabilities, and effectively equip our stakeholders to protect themselves and their patients.
8. **Greater transparency in the name of patient safety and privacy.** Along with increased collaboration, we anticipate seeing more medical device manufacturers transparently sharing vulnerabilities in the year ahead—not only because doing so aligns with the **HSCC Medical Device and Health IT Joint Security Plan (JSP)**, but also because transparency will no longer be taboo. Transparently sharing vulnerabilities will be a recognized best practice customers expect from all vendors who supply medical device technologies.

What drives us every day is our unwavering commitment to doing what is right for our customers and their patients. This is about protecting what matters most: patient privacy and patient safety. While the industry has made significant progress, there is work yet to be done. Whether you are a BD customer, industry regulator, threat intelligence organization, security researcher or fellow medical device manufacturer, we invite you to partner with BD to drive medical device cybersecurity forward. To learn more, visit the **BD Cybersecurity Trust Center**.

1 Health Sector Coordinating Council Joint Security Plan (JSP). Healthcare & Public Health Sector Coordinating Council. Accessed December 3, 2019. https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-Infographic.pdf

2 IBM Security and Ponemon Institute. 2019 Cost of a Data Breach Report. Published July 23, 2019. Accessed November 22, 2019. https://databreachcalculator.mybluemix.net/executive-summary. (Note: the 2019 report is available for download at: https://www.ibm.com/account/reg/us-en/signup?formid=urx-42215)

3 Lagasse J. Healthcare data breaches will cost industry $4 billion by year's end, and 2020 is poised to be worse. Healthcare Finance. Published November 4, 2019. Accessed March 11, 2020. https://www.healthcarefinancenews.com/news/healthcare-data-breaches-will-cost-industry-4-billion-years-end-and-2020-poised-be-worse

4 Lyons K. Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week. The Verge. Published April 16, 2020. Accessed August 25, 2020. https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams

5 Cybersecurity & Infrastructure Security Agency. People's Republic of China (PRC) targeting of covid-19 research organizations. Published May 13, 2020. Accessed August 25, 2020. https://www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations

6 Cybersecurity & Infrastructure Security Agency. Ransomware activity targeting the healthcare and public health sector. Published October 28, 2020. Updated November 2, 2020. Accessed November 4, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

7 Bing C, Menn J. Building wave of ransomware attacks strike U.S. hospitals. Reuters. Published October 28, 2020. Accessed October 30, 2020. https://www.reuters.com/article/us-usa-healthcare-cyber/building-wave-of-ransomware-attacks-strike-u-s-hospitals-idUSKBN27D35U

8 Center for Devices and Radiological Health. Premarket submissions: management of cybersecurity in medical devices. U.S. Food and Drug Administration. Published October 2018. Accessed Oct. 30, 2020. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices

9 Hewitt C. 5 ways to better manage medical device risk. Physicians Practice. Published September 27, 2019. Accessed March 11, 2020. https://www.physicianspractice.com/technology/5-ways-better-manage-medical-device-risk

10 Greig J. Cybercriminals unleash diverse wave of attacks on COVID-19 vaccine researchers. TechRepublic. Published June 17, 2020. Accessed September 8, 2020. https://www.techrepublic.com/article/cybercriminals-unleash-diverse-wave-of-attacks-on-covid-19-vaccine-researchers/

11 Landi H. Report: 40% of healthcare organizations hit by WannaCry in past 6 months. Fierce Healthcare. Published May 29, 2019. Accessed August 22, 2020. https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months

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

bd.com