2021 Cybersecurity Annual Report

Improving collaboration, transparency and cybersecurity resilience

BD
Advancing the world of health™

Protecting patient safety and privacy

A message from Rob Suárez, Chief Information Security Officer

In healthcare, cybersecurity is not just about protecting systems and data. There is a patient at the end of everything we do. That means cybersecurity is also a matter of patient safety. If a device cannot be used because of a cybersecurity attack, patient care and outcomes could be impacted. That is why we integrate cybersecurity into each phase of our product life cycle, from product design and development through supporting our products in use. By protecting the confidentiality, integrity and availability of BD products, manufacturing systems and enterprise IT, we are helping to improve the resilience of healthcare around the world.

Across BD, we are investing to innovate in three irreversible forces shaping the future of the healthcare industry: smart connected care, the transition to new care settings and improved chronic disease outcomes. As we develop new products and expand our offering of smart connected devices, we do so with cybersecurity at the forefront. Similarly, as we expand into new care settings, protections for those environments need to be as secure as the hospital setting.

At the same time, we recognize that the healthcare industry is the number one target for many cybercriminals. Since COVID-19 began, cyberattacks in healthcare have increased at an unprecedented rate, with threat actors using more sophisticated techniques, from specialized phishing attacks to ransomware. To protect the cybersecurity and resilience of BD and our products, we work with customers, vendors, industry regulators, stakeholders and security researchers. We invite you to learn more and partner with us as we continue to advance healthcare cybersecurity.

"By protecting the confidentiality, integrity and availability of BD products, manufacturing systems and enterprise IT, we are helping to improve the resilience of healthcare around the world."

State of healthcare cybersecurity

Since the beginning of the COVID-19 pandemic, cybersecurity threats against the healthcare industry have increased exponentially[1]. In 2020 alone, cyberattacks against healthcare endpoints increased 9,851% over the previous year[2], and nearly 28% of the cyberattacks executed against healthcare entities were ransomware attacks[3]. Further, the average data breach in hospitals and clinics between May 2020 and March 2021 cost $9.23 million, higher than any other industry[4].

While the healthcare industry has made strides in recent years toward advancing cybersecurity[5], risks remain prevalent. Hospital networks operate, on average, 350,000 medical devices at a time[6]. The sheer volume makes it challenging for healthcare IT professionals to manage the different types of threats that can impact the confidentiality, integrity and/or availability of medical devices. Add that the complexity of cyberattacks has also increased, as have the potential impacts to patients and hospital systems, and the stakes could not be higher. In healthcare, cybercriminals are working around the clock to:

- Disrupt the production and supply chain of medical technology
- Compromise healthcare data, including patients' protected health information
- Disrupt clinical workflows and the delivery of healthcare

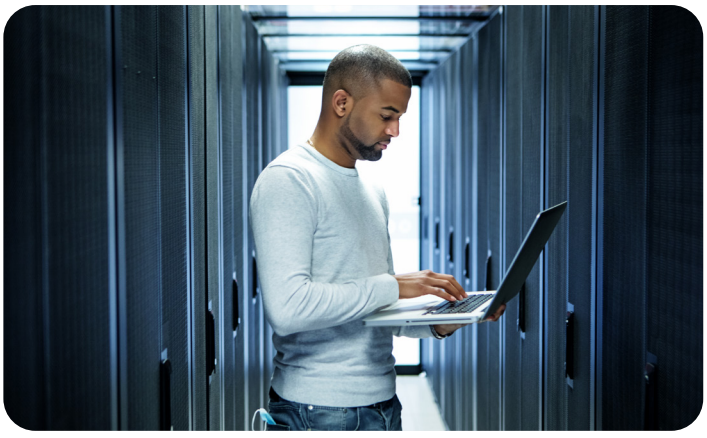
When it comes to ransomware, healthcare is one of the most targeted industries[7], with more than 100 documented attempts per week in the first half of 2021[8]. Traditionally, ransomware has involved infiltrating systems and then encrypting data and demanding a ransom payout for the decryption code. More recently, ransomware tactics have changed, and ransomware-as-a-service (RaaS) has become a standardized delivery model[9]. Similar to software-as-a-service (SaaS) offerings, RaaS is a subscription-based model that allows malicious individuals and groups to lease ransomware tools to execute ransomware attacks[10]. The ease and accessibility of this approach has contributed to the increase in ransomware attacks. In addition, many of the most recent high-profile attacks have come from ransomware groups, including nation state threat actors. Double- and triple-extortion attempts have also increased[11]. Double extortion involves threatening to publish exfiltrated data from systems infected by ransomware. Triple extortion involves demanding ransom payouts from third parties such as customers, partners or even patients[12].

Another tactic that has increased over the last year involves cybercriminals infiltrating an organization's network and staying hidden while they learn about the organization's backup processes. The attackers then disable those backup processes before initiating the ransomware attack, significantly reducing the organization's resilience[13]. Yet another tactic that has emerged involves cybercriminals threatening to destroy their victim's data and the decryption keys if the organization attempts to engage a ransomware negotiator[14].

These shifts demonstrate that ransomware attacks against healthcare are prolific and sophisticated. As a result, an increasing number of organizations are turning to cybersecurity insurance policies to offset potential costs associated with responding to and recovering from cyberattacks. However, cybersecurity insurance premiums have recently increased by as much as 50% in high-risk industries, while coverage limits are decreasing[15].

Additionally, while ransomware is often cited as healthcare's biggest cybersecurity threat[16], other risks — such as phishing, software vulnerabilities, insider threats and human error — can serve as gateway attacks, opening the door to ransomware.

Across the healthcare industry, the increasing sophistication of cybersecurity threats reinforces the need for transparency and collaboration between medical device manufacturers, healthcare providers, government agencies and the security industry. In this report, we will share our approach to protecting BD, our customers and our patients; information on how we collaborate to advance cybersecurity in healthcare; and cybersecurity trends we anticipate for 2022.



Cyber risks continue to evolve

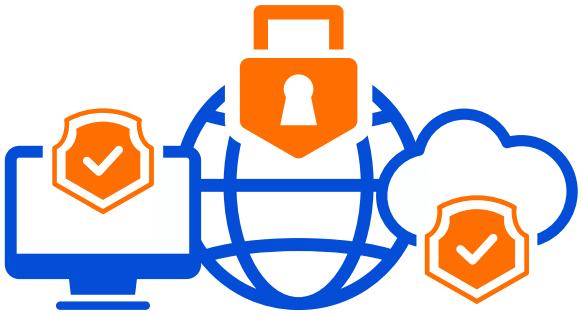
Cyber vulnerabilities and threats impact organizations of every size and in every location around the world. The following list highlights the range of cyber risks and threats organizations must guard against.

Internal risks

Software vulnerabilities – Software ages just like the human body. Instead of aches and pains, it develops weaknesses that can be exploited by cybercriminals to gain access to a computer system or its data. BD makes vulnerability disclosures and software patches available through the BD Cybersecurity Trust Center website, which was launched in December 2020. Customers can also receive software and patch updates remotely via our BD Remote Service and Support (RSS) solutions for supported products. When vulnerabilities are identified in third-party software components used in BD products, our R&D teams validate the associated patches before making them available to BD customers. Product security bulletins published to the BD Cybersecurity Trust Center also include compensating controls to enable customers and patients to more quickly mitigate potential risk.

Insider threats – Insider threats are malicious threats that come from within an organization, including current and former employees, contractors and partners. One type of insider threat is the unauthorized use of software, services or devices. BD protects against insider threats by educating our associates and monitoring for suspicious activity. We also limit the use of external storage devices, such as USBs and flash drives, and we perform comprehensive risk assessments on BD-approved applications to ensure they uphold rigorous security standards.

Human error – Mistakes such as unintentional policy violations are the root cause of many cybersecurity incidents. According to a recent survey conducted by the Healthcare Information and Management Systems Society (HIMSS), human error is the initial point of compromise 35% of the time when significant security incidents occur in healthcare[17]. BD reduces the risk of human error by training our associates and reinforcing BD Values, which include *We do what is right* and *We are all accountable*.



External threats

Phishing attacks – In healthcare, phishing remains the most common form of cyberattack[18]. Phishing is when criminals try to obtain sensitive information for the purpose of illegally accessing a computer or network. Their intent is to scam victims into revealing financial details, system credentials or other sensitive data so they can use that information to do things such as access password-protected systems, open new accounts or even launch ransomware attacks. BD maintains a monthly phishing simulation program to help our associates recognize and report suspicious emails. The program utilizes a simulation platform to track overall performance and point associates to additional training resources. In 2021, the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) performed an evaluation of our phishing simulation program and determined that this approach is mature, reliable and structured. Visit the CISA website for information about their cyber hygiene services.

Ransomware attacks – Ransomware is a type of malicious software (malware) that restricts access to a computer system until a demanded sum of money or cryptocurrency is paid. In healthcare, ransomware attacks that disrupt the availability of medical devices can cause life-threatening interruptions in patient care. Learn more about anti-malware protection built into BD products from our Product Security White Papers, which are available on the BD Cybersecurity Trust Center.

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. Our strategic approach to cybersecurity is based on three guiding principles:

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.

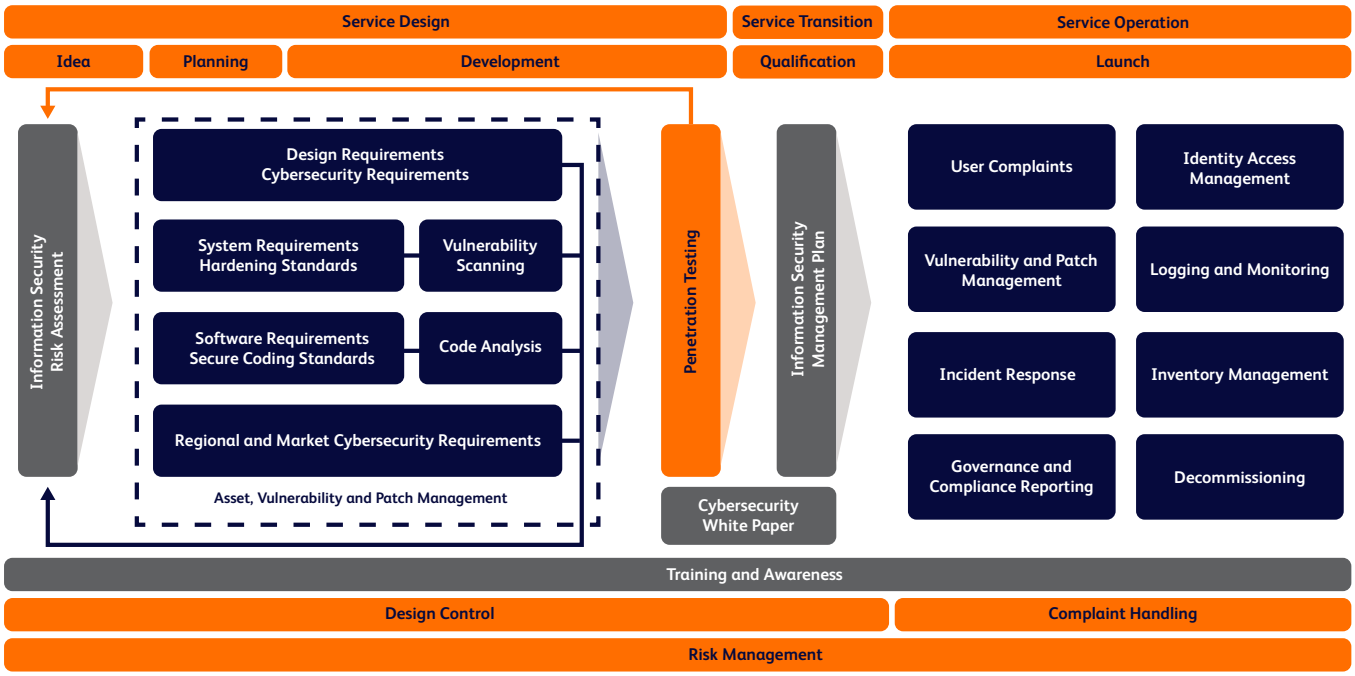
Security in use

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.

BD utilizes a framework to incorporate cybersecurity into our processes for product design, manufacturing, customer support and enterprise systems. Our framework has been aligned to various industry work products including the HSCC MedTech Joint Security Plan, NIST Cybersecurity Framework, ISO 27001, UL 2900 and ISA 62443.



Investing in cybersecurity

As new cybersecurity threats emerge, organizations must adapt their cybersecurity practices to continuously improve. The following 2022 initiatives exemplify our commitment to making BD products, manufacturing and IT more secure and resilient:

Across the Organization

- **Global Cybersecurity Operations Center (CSOC)** – BD operates a 24/7 global CSOC, which includes Operational Technology, and we are also investing in additional security operations resources in Greater Asia and EMEA for specialized initiatives, including regional alignment and alert investigations.
- **Cybersecurity certifications** – We are pursuing additional third-party cybersecurity certifications, including the U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC).

Product Security

- **Customer communications** – Extend the functionality of the BD Cybersecurity Trust Center to improve search capabilities and allow customers to sign up for automatic notifications.
- **Product development** – Continue to strengthen our product development capabilities to safeguard new and existing BD products, including smart connected devices. Identify continuous improvement opportunities in alignment with regulatory requirements for comprehensive threat modeling, routine software composition analysis and remediation, software-bill-of-materials disclosure, legacy product support and the adoption of state-of-the-art security controls.
- **Secure software development life cycle (SSDLC)** – Initiatives include application code signing for critical products, integrating secure DevOps into the R&D organization, and leveraging automation to strengthen the security of our software supply chain.

Manufacturing Security

- **Secure Operational Technology (OT)** – Continue to enhance cybersecurity capabilities for manufacturing and distribution centers with a focus on protecting OT systems used to monitor, control and manage industrial equipment, assets and processes.
- **Improve OT capabilities** – Expand our OT cybersecurity capabilities via a Center of Excellence and deploy multiple solutions, including asset inventory, OT risk management, OT network segmentation and remote access as part of our supply chain digitization strategy.

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 cloud and on premise and enhance protection against current and emergent cyberthreats.
- **Improve network visibility** – Strengthen capabilities for network visibility, access monitoring, anomaly detection and incident automation through advanced cybersecurity solutions.
- **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 passwordless authentication. This approach protects BD and our customers by managing and granting access based on the continuous verification of identities, devices and services.

Defending BD

BD proactively monitors for suspicious activity, including phishing attacks, malware attacks and insider threats. Phishing attempts against BD increased 78% during 2020 and increased by another 19% during the first half of 2021. In addition, our monitoring and detection team blocks an average of 14.4 million malicious activities per month.

14.4 million

BD blocks 14.4 million malicious activities per month.

Our cybersecurity program includes regular internal and external security assessments, penetration testing, threat intelligence, forensics and investigations, as well as vulnerability and incident management. We also leverage threat modeling to uncover and examine potential cybersecurity risks during the design process and beyond. To further ensure the efficacy of our cybersecurity program, our cybersecurity framework, policies and standards are reviewed annually for any potential updates and enhancements in collaboration with Risk Management, Internal Audit, Quality and impacted functions. These comprehensive assessments ensure that our cybersecurity policies and standards are applied consistently throughout the organization — and that they remain effective.

In addition, we provide cybersecurity awareness training to our approximately 75,000 associates comprised of online cybersecurity training modules; in-person and virtual cybersecurity bootcamp classes; Cybersecurity Awareness Month initiatives; monthly phishing simulation exercises; mock incident response exercises, including internal cybersecurity tabletop simulations that encompass product security, manufacturing security and IT security; and intranet resources aimed at enhancing associates' ongoing cyber awareness.

We do all of these things to protect BD products, manufacturing and IT systems — which in turn protect our patients and customers. We also work closely with our customers to help them use BD products securely and adapt with emerging best practices.

Adapt with emerging best practices

Cybersecurity hygiene measures help protect the confidentiality, integrity and availability of data and systems. However, as cyberthreats evolve, so must an organization's approach. At BD, we work with our customers and government agencies to help advance the understanding and adoption of industry best practices to strengthen cybersecurity and resilience. These include emerging best practices, such as:

Manage products over their intended life cycles

Connected medical devices must be maintained over time to be secure. This includes keeping operating systems current, patching known vulnerabilities and managing products over their intended life cycle. The challenge is that device usability often extends beyond its intended lifespan. However, end of life (EoL) and end of support (EoS) devices no longer receive critical cybersecurity updates and may be more vulnerable to cyberthreats. That is why clear communication about device cybersecurity is essential to empowering healthcare providers and patients to manage devices effectively.

At BD, we recognize that all software develops vulnerabilities over time. That is why we work closely with customers to enable BD products to be used in a secure environment. As a trusted partner, we provide guidance on proven best practices, including network segmentation and patch management. We also maintain Product Security White Papers for BD software-enabled products and make them available to customers through the BD Cybersecurity Trust Center. The purpose of these documents is to provide details on how BD security and privacy practices have been applied and what customers should know about maintaining security throughout the intended product life cycle. Additionally, each white paper includes a list of third-party software used in the device as well as detailed administrative, physical and technical safeguards and a Manufacturer Disclosure Statement for Medical Device Security (MDS2) attestation.

As new vulnerabilities are uncovered, BD makes security bulletins and patches available on the BD Cybersecurity Trust Center. Customers are encouraged to keep operating systems current and apply patches as they become available as part of managing products over their intended life cycles. In addition, customers are encouraged to upgrade to newer versions of medical devices over time and replace software and/or devices leveraging outdated technology that can no longer be secured.

BD Product Security White Papers

We maintain Product Security White Papers for software-enabled products and encourage customers to request them via the BD Cybersecurity Trust Center. These documents detail how security and privacy practices have been applied and provide information to help customers safeguard product security throughout each product's life cycle.

"We integrate cybersecurity into each phase of our product life cycle using the BD Cybersecurity Framework. We also work closely with customers to enable them to use BD products in a safe and secure environment and apply security updates as they become available. Upholding security throughout the medical device life cycle is essential to maintaining cybersecurity across all connected medical devices, whether they are considered new or represent legacy medical devices that have been in use for several years."

Scott Shindledecker
Chief Product Security Officer

Uphold rigorous cybersecurity standards for third parties

On average, healthcare providers have contracts with more than 1,000 third-party vendors[19]. Close to 50% of those third-party vendors typically have access to an organization's sensitive data[20]. However, according to the 2020 HIMSS Cybersecurity Survey, only 50% of healthcare organizations conduct comprehensive, end-to-end security risk assessments[21]. While the complexity of managing cybersecurity risk increases exponentially with a greater number of third-party vendors, healthcare providers can reduce that risk by conducting thorough risk assessments and ensuring that all third parties uphold rigorous cybersecurity standards.

At BD, new and existing technologies and systems are assessed against our cybersecurity framework and requirements. This allows us to identify potential gaps and risks associated with those technologies and systems, share that knowledge with customers, work to remediate those risks and ensure compensating controls are applied.

Engage independent cybersecurity evaluations

BD encourages healthcare providers to work with external third parties to test and validate their cybersecurity protocols at least annually. These evaluations can provide valuable insight about an orginization's cybersecurity posture, resilience and areas for improvement.

At BD, we recognize the value of independent cybersecurity attestations. Each year, a range of external third parties independently assess BD products and internal cybersecurity controls. To demonstrate our commitment to product security and the protection of customer data, we share these industry-recognized certifications and attestation reports through the BD Cybersecurity Trust Center. These include Underwriters Laboratories Cybersecurity Assurance Program (UL CAP) certifications and SOC2+ reports for a variety of software-enabled products.

Build a robust community of practice

Conservative estimates suggest that more than 75% of hospitals around the world lack sufficient cybersecurity expertise on staff[22]. This makes the challenge of managing thousands of medical devices even more difficult. We integrate cybersecurity into each phase of our product life cycle, and we also recognize the importance of developing a strong community of practice to advance cybersecurity in healthcare.

With new cybersecurity threats emerging daily, a strong community of practice must include information sharing. We augment our own threat intelligence gathering by partnering with industry, government and law enforcement organizations for additional threat intelligence information. These include organizations like:

- **The Domestic Security Alliance Council** (DSAC), a strategic alliance that includes the U.S. Federal Bureau of Investigation (FBI), U.S. Department of Homeland Security (DHS) and private industry networking together to increase security.
- **The Health Information Sharing and Analysis Center** (H-ISAC), shares coordinated vulnerability disclosures impacting software used in medical devices, including BD devices.
- **National Cyber-Forensics and Training Alliance** (NCFTA), a nonprofit partnership between private industry, government and academia that enables collaboration for the purpose of identifying, mitigating and disrupting cybercrime.
- **New Jersey Biotechnology Threat Focus Cell**, a local branch of the FBI that is focused on the biotechnology industry and hosts a monthly threat intel exchange aimed at sharing credible threat intel among industry members, in partnership with other federal agencies.

We also engage the security research community through events like the Biohacking Village Medical Device Lab, a 501(c)3 organization that brings medical device manufacturers and security researchers together to strengthen medical device security. Each year, medical device manufacturers submit medical devices to the Biohacking Village Medical Device Lab with information about the context in which they are used. Security researchers then learn about those devices and test them for previously unknown vulnerabilities. As a manufacturer, events like the Biohacking Village allow us to tap into a varied set of skills and experiences in a controlled environment. While we do our own penetration testing and threat modeling, we welcome vulnerability reports from security researchers, as well as BD customers, third-party component vendors and other external groups.

Vulnerability disclosure

When we receive a report of a vulnerability in a BD software-enabled device, we partner with the issue reporter to assess and confirm the vulnerability. Once confirmed and validated, we issue a coordinated vulnerability disclosure. For maximum awareness, BD voluntarily reports vulnerabilities to the U.S. Food and Drug Administration (FDA) and Information Sharing Analysis Organizations (ISAOs) where BD participates, including the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the Health Information Sharing and Analysis Center (H-ISAC). Additionally, BD follows the FDA's Postmarket Management of Cybersecurity in Medical Devices guidance to properly communicate vulnerabilities to BD customers.

BD has established a routine practice of seeking, communicating and addressing cybersecurity issues associated with our products in a timely fashion. BD was one of the first medical device manufacturers to develop a mature coordinated vulnerability disclosure program. We recognize that customers cannot protect their systems and their patients from cybersecurity threats they do not know about. That is why we believe transparency and collaboration are essential.

Visit the BD Cybersecurity Trust Center to access product security bulletins and patches or to learn more about our coordinated vulnerability disclosure process. Current and prospective customers can also request Product Security White Papers.

"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. We view coordinated disclosure as a sign of maturity of an organization, and we follow the FDA guidance to properly communicate vulnerabilities to BD customers, enabling them to manage risk properly through awareness and guidance. We also make a number of cybersecurity templates available through the BD Cybersecurity Trust Center to help customers and fellow medical device manufacturers develop strong coordinated vulnerability management processes."

Nastassia Tamari
Director, Information Security – Operations

Collaborate effectively to advance cybersecurity in healthcare

Healthcare cybersecurity is a joint effort that requires collaboration between medical device manufacturers, healthcare organizations, third-party vendors, industry regulators and security researchers. BD maintains a culture of transparency and collaboration with customers and industry stakeholders to establish industry best practices and address emerging cybersecurity risks. The following engagements reflect our contribution to advancing cybersecurity across the industry in 2021.

AdvaMed Cybersecurity Working Group

Chaired by BD CISO Rob Suárez, this working group contributed to a number of industry discussion papers, including the National Telecommunications and Information Administration (NTIA) report on The Minimum Elements for a Software Bill of Materials (SBOM), published in July 2021, pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity, issued in May 2021 by U.S. President Biden. The working group also provided comments on identifying and managing bias in artificial intelligence and strengthening cybersecurity practices associated with servicing medical devices.

Biohacking Village at DEF CON

BD was one of the original medical device manufacturers to contribute to the Biohacking Village Medical Device Lab at DEF CON. In 2021, we submitted BD Pyxis™ IV Prep, a guided, gravimetrics-based IV Workflow Management System (IVWMS) designed to support pharmacy compounding operations. Security researchers at the Biohacking Village were given opportunities to try and access a sample drug database within a simulated environment. No evidence of compromise was found by the end of the three-day event. In addition, BD CISO Rob Suárez spoke during the 2021 Biohacking Village about the value of engaging with security researchers in a crowdsourced approach to strengthen medical device security.

CVE Program

In June 2021, BD became the first medical technology company authorized as a Common Vulnerability and Exposures (CVE®) Numbering Authority by the CVE Program. This means that BD is now authorized to assign CVE identification numbers to newly-discovered vulnerabilities in its software-enabled products. This includes using the Common Weakness Enumeration (CWE™) system to classify vulnerability types and applying the Common Vulnerability Scoring System (CVSS) to communicate vulnerability characteristics and severity. The CVE Program is sponsored by the Cybersecurity and Infrastructure Security Agency (CISA) and operated by MITRE Corporation.

HSCC Cybersecurity Working Groups

The Healthcare and Public Health Sector Coordinating Council (HSCC) includes multiple cybersecurity working groups. BD co-chairs the International Engagement Task Group and participates in the MedTech Vulnerability Communications Working Group and the Sample Communications Sub-Group, which is working to create scalable communication guidelines to help medical device manufacturers communicate more effectively with customers and patients regarding software vulnerabilities in medical devices.

IMDRF Cybersecurity Working Group

BD helped draft an international guidance on software-bill-of-materials (SBOM) for the International Medical Device Regulators Forum (IMDRF) Cybersecurity Working Group. Our contribution focused on best practices for operationalizing transparency throughout the life cycle of each medical device. This included advice on how different types of software components can be inventoried during the software development life cycle, tools that can be leveraged and how to manage and maintain an actionable SBOM repository for publication and distribution.

MDIC Cybersecurity Working Group

BD participated in several Medical Device Innovation Consortium (MDIC) initiatives in 2021. BD CISO Rob Suárez chaired the MDIC Cybersecurity Working Group, which launched the Medical Device Cybersecurity Maturity Survey in collaboration with the HSCC. The purpose of the survey is to establish a benchmark of the medical device industry's cybersecurity maturity so that healthcare providers and medical device manufacturers can plan for and track their progress toward advancing cybersecurity maturity over time.

In 2021, BD also helped facilitate the MDIC Virtual Threat Modeling Bootcamp series for medical device stakeholders and contributed to the organization's Playbook for Threat Modeling Medical Devices, released in November 2021 in collaboration with MITRE Corporation. BD is also actively contributing to the MDIC medical device penetration workgroup that focuses on developing best practices and making recommendations on how this technique best fits in a regulated medical device environment.

MTE Cybersecurity Working Group

BD participated in the MedTech Europe (MTE) Cybersecurity Working Group (CWG). Through the CWG, cybersecurity experts engage with European institutions, including the European Union Agency for Cybersecurity (ENISA), to offer industry input on relevant policy matters and build the MedTech industry's voice. BD actively contributed to expressing MTE's position and voice through consultations and represented MTE in ENISA's Stakeholder Cybersecurity Certification Group (SCCG).

Trinity Challenge

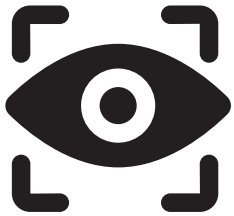
During the technology section of the Trinity Challenge, BD participated with the Royal Society and the International Digital Health and Artificial Intelligence Research Collaborative (I-DAIR) in an engaging discussion about how to improve safe data access for health emergencies like the COVID-19 pandemic, which helped to shape the agenda for the G7 discussion on artificial intelligence in healthcare post-COVID. Our contribution included use cases and real-world examples of how the G7 can come together to better prepare for access to data through artificial intelligence/machine learning, privacy and public-private partnerships.

CISA

BD collaborates with the Cybersecurity and Infrastructure Security Agency (CISA) to provide information about vulnerabilities in BD products. CISA also partners with organizations like BD to perform phishing simulation campaign assessments and cyber resilience review (CRR) assessments. In 2021, we partnered with CISA to assess our internal phishing simulation program to ensure that we properly equip associates to identify and report phishing emails. We also collaborated with CISA to assess our manufacturing and operating technology system cybersecurity and resilience, which is essential to fulfilling our Purpose of *advancing the world of health*™.

Future trends

The healthcare industry has seen significant change in the last year, including the resurgence of COVID-19 infections and a global vaccination campaign, while cybercriminals remained persistent in their attacks. Here are the cybersecurity trends we anticipate for 2022.



1. **More software providers will use digital code-signing capabilities.** One of the biggest cyberattacks that made headlines in 2021 was SolarWinds, which began when cybercriminals inserted malicious code into an update for SolarWinds Orion software[23]. As a result, we expect to see code-signing procedures scrutinized more carefully. In addition, more companies that develop software will leverage digital code-signing certificates to validate software code authenticity to their customers and users.
2. **Medical device manufacturers will prepare for software-bill-of-materials (SBOM) requirements to take effect.** Even before new requirements take effect, medical device manufacturers will prepare for SBOM requirements and will go to greater lengths to inform customers and patients about the software components used within each medical device. This visibility will help healthcare providers and medical device manufacturers execute more efficient incident management processes.
3. **More healthcare organizations will perform risk assessments on third-party vendors.** Security questionnaires and cyber risk scores are frequently used to evaluate third-party vendors during the procurement process. However, they may not address emerging cybersecurity risks or provide sufficient detail about third-party vendors' security practices. Looking ahead, we expect to see more healthcare organizations performing comprehensive risk assessments on all third parties that have access to sensitive data.
4. **Customer and patient communication will continue to improve.** It is not just healthcare providers who need visibility into software components and awareness of potential vulnerabilities. Patients need this information too. As we look ahead to 2022, we will see more medical device manufacturers taking multiple audiences into consideration when crafting technical documentation and vulnerability communications. This communication is so important that the U.S. Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH) issued Best Practices for Communicating Cybersecurity Vulnerabilities to Patients in October 2021. While the document does not represent formal guidance, it illustrates the criticality of transparency and collaboration between medical device manufactures and patients, as well as healthcare delivery organizations.
5. **Across the healthcare industry, organizations will prioritize cybersecurity awareness.** Employees are often the first line of defense in thwarting cybersecurity attacks. Moving forward, we will see organizations offer more comprehensive cybersecurity awareness training.
6. **More healthcare organizations will participate in independent cybersecurity assessments.** External third parties can provide valuable insight and validate the benefits of investing in cybersecurity advances. From engaging agencies like CISA to working with private third-party cybersecurity firms, we anticipate an increase in healthcare organizations leveraging independent cybersecurity assessments during the coming year.
7. **More organizations in healthcare will engage in cyber simulation activities.** Tabletop exercises and cyber war games allow organizations to plan for cyberattacks and assess their ability to respond effectively. In 2022 and beyond, more healthcare providers and medical device manufacturers will leverage cyber simulation activities to ensure their associates, executive leaders and board members are equipped before an attack happens.

Trends we will continue to see moving forward

BD introduced the following cybersecurity trends in its inaugural cybersecurity annual report from 2020, and we expect them to continue well into 2022 and beyond:

- **Ongoing challenges related to remote work.** Healthcare organizations will likely continue to offer remote work options and increased access to telehealth. Therefore, the challenges associated with securing remote workers' connectivity and data will also continue.
- **An increase in ransomware attacks against healthcare providers.** More than a third of healthcare organizations became victims of ransomware attacks in 2020[24]. Among those not impacted by ransomware, 41% report that they expect to receive ransomware in the future[25]. Given the pace of attacks and the accessibility of ransomware-as-a-service (RaaS) tools, we anticipate that ransomware attacks against healthcare providers will continue to increase.
- **Expanded adoption of Zero Trust principles.** While Zero Trust principles — the practice of trusting no one by default and operating as though the network has already been compromised — have gained momentum across all industries, 65% of organizations have yet to adopt a Zero Trust approach[26]. Given that the average cost of a data breach in healthcare has increased 29.5% in the last year and taking a Zero Trust approach can reduce that cost[27], we expect to see more healthcare organizations embrace Zero Trust principles in the future.

At BD, even while we seek to increase robust cybersecurity measures across the healthcare industry, we continuously enhance our own cybersecurity practices to protect BD products, manufacturing and IT — which in turn protect our patients and customers. In everything we do, we are committed to improving the resilience of healthcare. We invite you to partner with BD in this effort to advance cybersecurity maturity and resilience. To learn more, visit the BD Cybersecurity Trust Center.

1 Landi H. Relentless cyberattacks are putting financial pressure on hospitals: Fitch Ratings. Fierce Healthcare. https://www.fiercehealthcare.com/tech/relentless-cyber-attacks-are-putting-pressure-hospital-finances-fitch-ratings. Published on July 26, 2021. Accessed on August 17, 2021.

2 United States Department of Health and Human Services (HHS). 2020: A Retrospective Look at Healthcare Cybersecurity. Accessed on August 19, 2021, at https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf.

3 IBM Security. X-Force Threat Intelligence Index 2021. https://www.ibm.com/security/data-breach. Accessed on July 26, 2021.

4 IBM Security. How much does a data breach cost? https://www.ibm.com/security/data-breach. Accessed on November 10, 2021.

5 Jercich K. Hospitals lag other companies in cybersecurity risk ratings. Healthcare IT News. https://www.healthcareitnews.com/news/hospitals-lag-other-companies-cybersecurity-risk-ratings. Published on August 5, 2021. Accessed on August 19, 2021.

6 Rozumalski K. Working together to secure our expanding connected health future. Help Net Security. https://www.helpnetsecurity.com/2020/10/06/working-together-to-secure-our-expanding-connected-health-future/. Published on October 6, 2020. Accessed on August 17, 2021.

7 Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority. Coveware. https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority. Published on July 23, 2021. Accessed on August 17, 2021.

8 Bracken B. Ransomware's New Swindle: Triple Extortion. Threat Post. https://threatpost.com/ransomwares-swindle-triple-extortion/166149/. Published on May 14, 2021. Accessed on August 17, 2021.

9 United States Department of Health and Human Services (HHS). 2020: A Retrospective Look at Healthcare Cybersecurity. Accessed on August 19, 2021, at https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf.

10 Ransomware as a Service (RAAS) Explained. Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/. Published on January 28, 2021. Accessed on August 17, 2021.

11 Bracken B. Ransomware's New Swindle: Triple Extortion. Threat Post. https://threatpost.com/ransomwares-swindle-triple-extortion/166149/. Published on May 14, 2021. Accessed on August 17, 2021.

12 Bracken B. Ransomware's New Swindle: Triple Extortion. Threat Post. https://threatpost.com/ransomwares-swindle-triple-extortion/166149/. Published on May 14, 2021. Accessed on August 17, 2021.

13 Vaidya A. Hive is a new & potentially devastating type of ransomware. Here's what you need to know. MedCity News. https://medcitynews.com/2021/09/hive-is-a-new-potentially-devastating-type-of-ransomware-heres-what-you-need-to-know/. Published on September 16, 2021. Accessed on September 17, 2021.

14 Olenick D. Is Grief's Threat to Wipe Decryption Key Believable? GovInfoSecurity. https://www.govinfosecurity.com/griefs-threat-to-wipe-decryption-key-believable-a-17556. Published on September 16, 2021. Accessed on September 17, 2021.

15 Lerman R. Ransomware claims are roiling an entire segment of the insurance industry. *The Washington Post*. June 17, 2021. Accessed on November 17, 2021, at https://www.washingtonpost.com/technology/2021/06/17/ransomware-axa-insurance-attacks/.

16 Davis J. Biggest Healthcare Security Threats, Ransomware Trends into 2021/. Health IT Security. https://healthitsecurity.com/features/biggest-healthcare-security-threats-ransomware-trends-into-2021. Published on December 18, 2020. Accessed on September 27, 2021.

17 2020 HIMSS Cybersecurity Survey. Healthcare Information and Management Systems Society (HIMSS). https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf. Accessed on October 4, 2021.

18 Cybersecurity and Security Incidents in Healthcare Infographic. Healthcare Information and Management Systems Society (HIMSS). https://www.himss.org/resources/cybersecurity-and-security-incidents-healthcare-infographic. Published on July 6, 2021. Accessed on September 27, 2021.

19 Ponemon Institute. The Economic Impact of Third-Party Risk Management in Healthcare. https://censinet.com/wp-content/uploads/2019/07/Ponemon-Censinet-Survey-Report-third-party-vendor-risk-management-research-economic-impact-v2-1.pdf. Published in July 2019. Accessed on August 5, 2021

20 Keskin OF, Caramancion KM, Tatar I, et. al. Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics*. 2021; 10(10):1168. doi: 10.3390/electronics10101168

21 2020 HIMSS Cybersecurity Survey. Healthcare Information and Management Systems Society (HIMSS). https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf. Published on November 16, 2020. Accessed after April 19, 2021.

22 Davis J. 87% Health Orgs Lack Security Personnel for Effective Cyber Posture. Health IT Security. https://healthitsecurity.com/news/87-health-orgs-lack-security-personnel-for-effective-cyber-posture. Published on March 5, 2020. Accessed on September 27, 2021.

23 Oladimeji A. SolarWinds hack explained: Everything you need to know. TechTarget. https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know. Published on June 16, 2021. Accessed on August 24, 2021.

24 Pifer R. More than 1/3 of health organizations hit by ransomware last year, report finds. HealthcareDive. https://www.healthcaredive.com/news/more-than-13-of-health-organizations-hit-by-ransomware-last-year-report-f/602329/. Published on June 24, 2020. Accessed on September 22, 2021.

25 Pifer R. More than 1/3 of health organizations hit by ransomware last year, report finds. HealthcareDive. https://www.healthcaredive.com/news/more-than-13-of-health-organizations-hit-by-ransomware-last-year-report-f/602329/. Published on June 24, 2020. Accessed on September 22, 2021.

26 IBM Security. X-Force Threat Intelligence Index 2021. https://www.ibm.com/security/data-breach. Accessed on July 26, 2021.

27 IBM Security. X-Force Threat Intelligence Index 2021. https://www.ibm.com/security/data-breach. Accessed on July 26, 2021.

BD Franklin Lakes, NJ 07417 U.S.

bd.com

BD
Advancing the world of health™