Canon

Cybersecurity Solutions

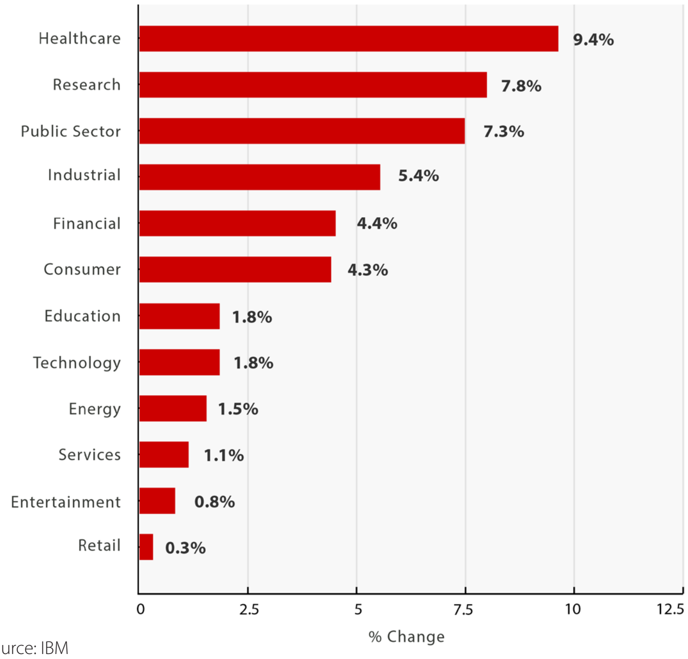
A Look at Protection
in the Digital Age

Safeguarding Diagnostic Imaging Technologies From Systemic Cybersecurity Breaches.

Healthcare organizations are particularly prone to cyberattacks as they possess information high in monetary and intelligence value, such as Personal Health Information (PHI) and Personally Identifying information (PII). In 2023, the average cost of a healthcare breach was almost $11 million—the highest compared to any other industry. That is a 53% increase over 2020.[1]

The rapid digital transformation in the healthcare industry driven by government initiatives has brought numerous benefits, but also exposed healthcare organizations to cybersecurity risks.

Increase in Average Cost of Data Breach by Industry 2021-2022



Source: IBM

The impact of cyber threats on healthcare organizations goes beyond compromising patient care. It can result in financial losses, reputational damage, erosion of patient trust, potential legal consequences, and in some instances irrevocable damages.

To address these challenges, implementing cybersecurity solutions to protect their digital infrastructure is a must for healthcare organizations.

> *Cyber safety is patient safety.*
>
> **ERIK DECKER CHAIRMAN**
> *Cybersecurity Working Group of the Health Sector Coordinating Council Vice President, Chief Information Security Officer, Intermountain Health*[3]

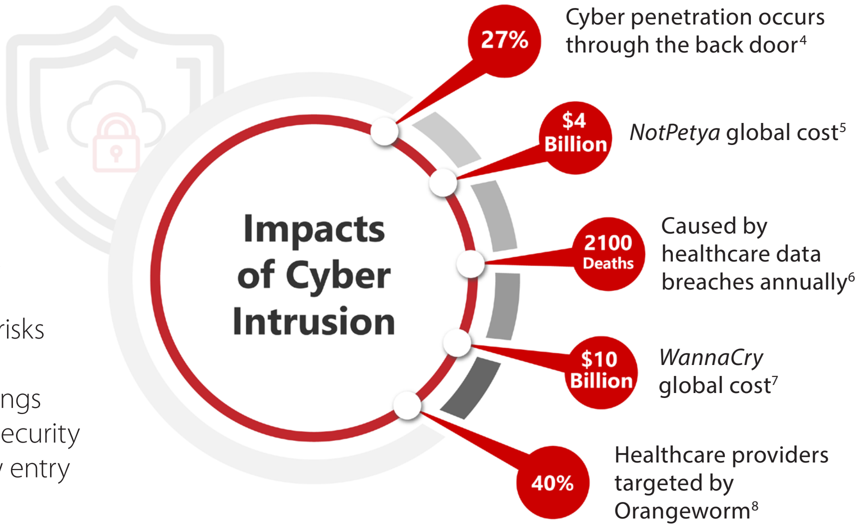
Canon Medical is here to help you navigate the complexities of the digital age. We offer robust Federal Information Processing Standards (FIPS) certified, multi-tiered standard and premium cybersecurity solutions that help protect your medical imaging devices by mitigating cyber threats, as well as your patients.

Our dedicated global cybersecurity risk management team is committed to ensuring Canon Medical is current with the latest cybersecurity regulations and industry security standards so you can rest assured your assets are receiving the best possible protection.

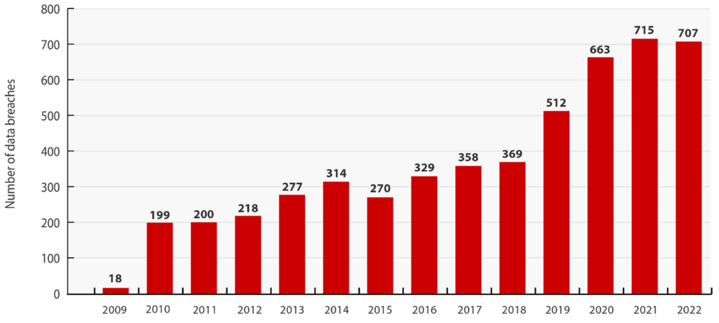
Taking a Closer Look At Ever-Changing Cyber Tactics

The current cybersecurity landscape experiences constantly evolving and increasingly sophisticated threats. Cyber attackers continuously develop new tactics to breach security defenses and gain unauthorized access to sensitive information. Ransomware attacks have gained significant attention recently, with high-profile incidents affecting various industries, including healthcare, finance, and government.

These attacks involve encrypting critical data and demanding ransom payments in exchange for its release, causing disruption, financial losses, and reputational damage. Ransomware attacks, phishing, social engineering, and malware pose significant risks to patient data and healthcare operations. The Internet of Things (IoT) further complicated the security landscape by introducing new entry points for cybercriminals.


Impacts of Cyber Intrusion
27%
Cyber penetration occurs through the back door[4]
$4 Billion
NotPetya global cost[5]
2100 Deaths
Caused by healthcare data breaches annually[6]
$10 Billion
WannaCry global cost[7]
40%
Healthcare providers targeted by Orangeworm[8]

According to a recent study by the University of Minnesota and the University of Florida, “the annual number of ransomware attacks on healthcare delivery organizations more than doubled from 2016 to 2021, exposing PHI of over 40 million patients.”[9] The study also noted the most common disruptions were electronic system downtime, cancellations of scheduled care, and ambulance diversion.



Number of healthcare data breaches involving the loss of 500 or more records in the United States from 2009 to 2022[10]

How Did Healthcare Institutions Become So Vulnerable to Cyber Threats?

The American Recovery and Reinvestment Act (ARRA) of 2009 attempted to address economic challenges to digitizing systems for healthcare providers. At the time of its passing, the U.S. economy was in the throes of a major recession. As part of the solution, the elected administration created the Health Information Technology for Economic and Clinical Health (HITECH) Act for ARRA. It codified the creation of the Office of the National Coordinator for Health IT (ONC). The HITECH Act provided the initial funding to incentivize providers to digitize health records. It enabled the development of system architecture to support healthcare delivery reforms championed by Congress in what we would see later in the passage of the Patient Protections and Affordable Care Act (ACA) of 2010.

Within an 18-month window, providers had to make critical decisions in choosing electronic health records technology vendors to ensure they would qualify for federal payments. According to Kaiser News and Fortune magazine, over 700 vendors offered their proprietary software solutions to assist healthcare providers in meeting the ONC requirements.

The government’s intention to establish a digital footprint in healthcare was necessary, but the execution could have been better. The rush to meet federal benchmarks and secure incentive payments led to the emergence of underdeveloped products and little emphasis on cybersecurity.

Many software developers created products aligned with the stimulus requirements but failed to address the intended goals of connectivity, interoperability, and the security of patients’ health records. As a result, the healthcare industry became vulnerable to cyber threats.

The Omnibus Appropriations Bill was passed in January 2023, providing funding and authority to the FDA for regulating cybersecurity in medical devices. This decision could transform healthcare cybersecurity by focusing on securing medical devices from the outset.

The Larger Impact of Cybersecurity on Healthcare Organizations

The effects of patient privacy breaches within healthcare organizations continue to be far-reaching and detrimental. When patient data falls into the wrong hands, it may be used for various malicious activities, including identity theft, insurance fraud, or even blackmail. Compromised medical records can lead to incorrect diagnoses, inappropriate treatments, or delays in critical care, jeopardizing patient safety and well-being.

Recent Examples of Cyberattacks Implications on Healthcare Institutions

Shields Health Care Group, a Massachusetts-based medical services provider fell victim to the largest data breach of April 2023. Reports emerged near the end of the month that a cyber criminal had gained unauthorized access to the organization's systems and had stolen personal data, billing information, insurance numbers and other financial details of 2.3 million people in the attack.[13]

A ransomware attack at The University of Vermont Medical Center on October 28, 2020, led to losing access to network intranet servers, email communications, and clinical systems. They took electronic medical records (EMR) offline, causing a loss of access to important production records. They also turned off the internet, VPNs, and integrations and took the EHR offline as a proactive measure. It took 40 days to succeed in the nearly complete restoration of their systems.[11]

In 2023, Idaho Falls Community Hospital, Mountain View Hospital, and nearby partner clinics had to redirect ambulances due to a cyberattack. Clinicians at Idaho Falls Community Hospital resorted to using paper charts, while some connected clinics remain closed.[8] **This illustrates the unfortunate ripple effects of successful cyber attackers who completely disrupt operations at multiple healthcare centers, denying patients critical care—and at high costs to healthcare organizations.**[14]

In October 2022, a breach at CommonSpirit Health cost them an estimated $160 million. Nontargeted hospitals within the community are also affected. A study coined this type of impact situation "a regional disaster."[12]

Regional healthcare organizations and larger health systems may struggle with reputational damage, erosion of patient trust, and potential legal repercussions, resulting in significant financial losses. Some cyber breaches have been so dire that they forced the closure of freestanding imaging centers and physician offices because of an inability to meet the requirements of the ransomware. These closures are truly unfortunate, given the need for these access points for healthcare services within local communities.

Counting the Costs: The Financial Toll

Unfortunately, the impact of cyber-attacks goes beyond jeopardizing patient care. They also have severe cost implications for healthcare organizations. They impact the efficiency of revenue cycles and delay electronic claims decisions, forcing a return to slower manual processes on paper. As a result, organizations experience a decline in days cash-on-hand metrics, as the IT system remains inaccessible until they've resolved cyber ransoms.

> *Of the organizations that reported losses from a ransomware attack, more than two-thirds (67%) said their combined losses reached between $1 million and $10 million while 4% estimated staggering losses in the range of $24 million to $50 million.*[15]

On July 26, 2023 the SEC adopted a new rule requiring public companies to disclose material breaches within four days. In addition, an annual disclosure in which public companies must disclose their cybersecurity processes is also mandated.[16]

Ultimately, investing in robust cybersecurity measures and proactive defense strategies is crucial to mitigate these costs and protect the financial stability of healthcare organizations.

Healthcare Leaders Agree: Cybersecurity = Top Priority

To build a resilient and equitable healthcare system, we need to address the pressing issues of interconnected infrastructure and the need for robust cybersecurity solutions—down to the equipment level. By taking on these challenges, we can forge a future where medical device companies work hand-in-hand with healthcare organizations using cybersecurity solutions that create a resilient and secure healthcare landscape.

Healthcare leaders agree. A recent survey conducted by Porter Research revealed a rare occurrence: unanimous agreement among business leaders in the provider, payer, and pharmaceutical/life sciences industries. They identified "growing hacker sophistication" as the primary driver behind the surge in ransomware attacks, including cybercriminals impersonating government agencies. The American Hospital Association acknowledged cybercriminals' increasing organization and skill level, underscoring the need for enhanced security measures.[17]

Last year, Canon met with hospital executives to discuss hospitals' challenges in seeking payments from insurance companies to cover novel procedures. The conversation pivoted toward the most significant challenges and concerns that hospital providers face today, other than payment obstruction by the payer community—the resounding answer was Cybersecurity.

"That was the response from all executives in attendance," said Tom Szostak, Director of Healthcare Economics at Canon Medical. "The credit card interface in the hospital's cafeteria was ripe for a hacker's entry into the financial system that infiltrated the entire IT network. Within seconds, registration at the main lobby and emergency room locked up. The result was the rapid spread of a cyber virus that shut down the hospital network for nearly a week."

Overall, industry experts consider it a necessary step, long overdue, to enhance cybersecurity in the healthcare industry.[18] This includes the emphasis on medical device manufacturers' responsibility to ensure device security and provide support to meet new government requirements.

Protect Your Investments

When developing our diagnostic imaging technologies, Canon Medical is hyper-focused on ensuring that all our imaging systems are free from cyber threats to the medical community. We know we have a responsibility to protect healthcare organizations and their patients.

> *Of all deployments that incorporate the Canon Medical Cybersecurity Firewall, not a single imaging device has been breached.*

Cybersecurity Risk Management Team

Our dedicated cybersecurity risk management team performs regular testing and evaluation of systems for vulnerabilities, develops and maintains cybersecurity regulations and standards, responds to security incidents, and streamlines security procedures. The team continually reviews the latest cyber risks and provides support to help your business react to potential hazards. Customers can also receive rigorous risk assessments and proactive threat monitoring from our dedicated worldwide task force, collaborating to discuss vulnerabilities and similar requests. With our expertise, Canon Medical Systems is the first OEM to achieve Authorization to Operate (ATO) with Air Force for Diagnostic Imaging equipment.

Canon's cybersecurity solutions are built on years of expertise and a deep understanding of the healthcare landscape, including sophisticated cyberattacks. They provide a multi-layered approach to safeguarding critical healthcare infrastructure and important information. Customers receive robust technologies, industry best practices, and proactive security measures to mitigate risks to the confidentiality, integrity, and availability of sensitive information and digital infrastructure.

Canon helps our customers tailor cybersecurity solutions to the specific needs of their healthcare organization. With standard solutions that every customer enjoys through Canon Medical Service contracts, to premium solutions that further enhance protection, Canon Medical is able to address many cybersecurity concerns including:

Endpoint Protection

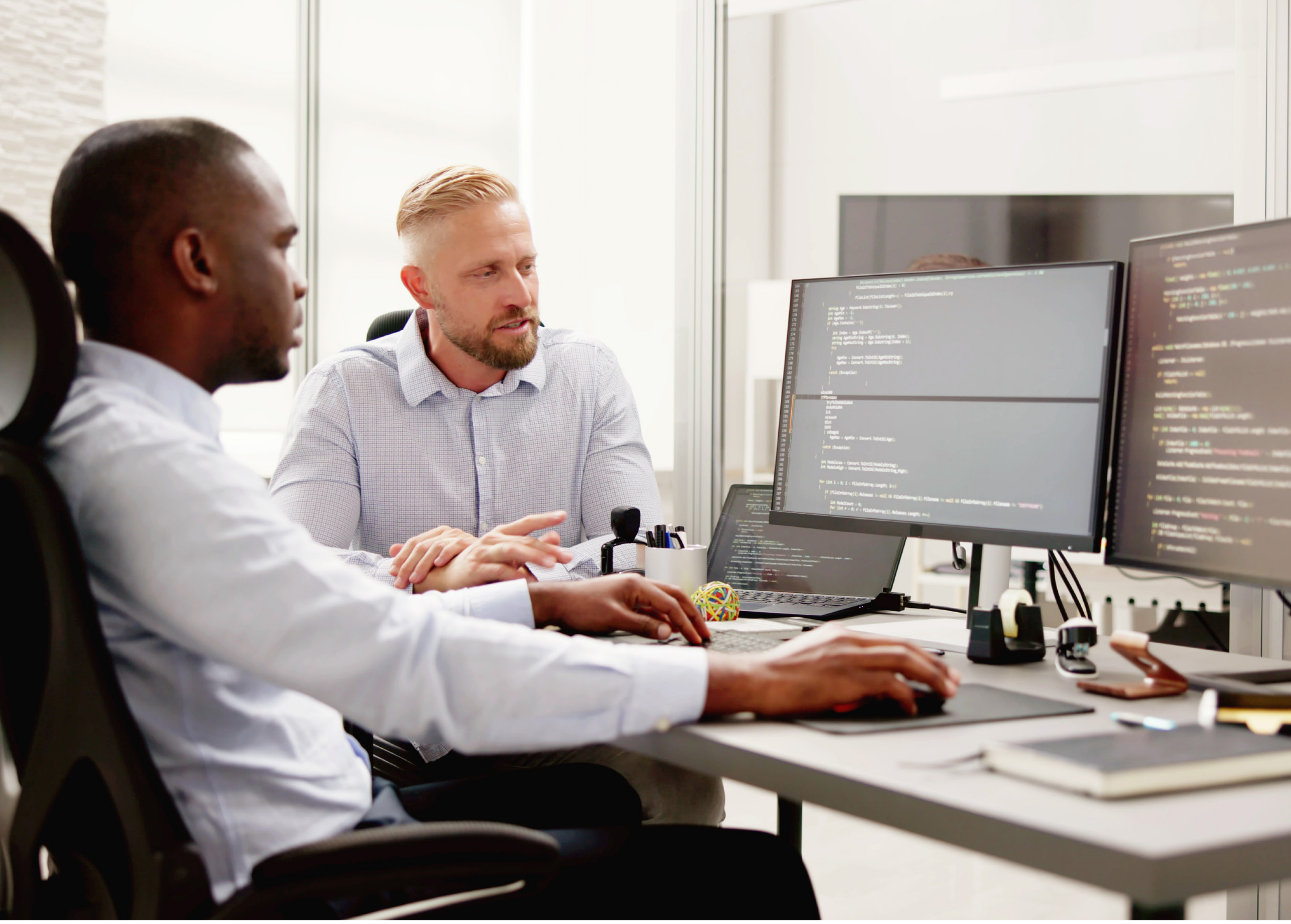
Recognizing the vulnerability of medical devices and endpoints within healthcare organizations, both solutions incorporate advanced endpoint protection. These mechanisms safeguard against malware, unauthorized modifications, and potential exploitation of vulnerabilities in medical devices.

Network Security

Security measures protect against unauthorized access, malware, and other network-based threats. By implementing secure network architectures and leveraging encryption technologies, they help maintain the confidentiality and integrity of patient data.

Data Encryption

Strong encryption protocols protect sensitive patient information at rest and in transit. Encryption ensures that even if data is intercepted or accessed without authorization, it remains indecipherable and unusable to unauthorized individuals.



Canon prioritizes minimal disruption to existing workflows while enhancing security measures and system efficiency. Cybersecurity Standard and Premium are also designed to integrate smoothly into various healthcare infrastructures, including electronic health record (EHR) systems, medical imaging platforms, and other critical components. Most importantly, our cybersecurity solution isolates our imaging systems from any network attack.

Amid the digital transformation of healthcare, we envision a better and more secure landscape where organizations can embrace technological advancements while effectively managing cybersecurity risks. At Canon Medical, we understand the crucial role of cybersecurity in the healthcare industry, and we are committed to working alongside our customers to safeguard their medical devices from potential breaches.

By partnering with Canon Medical and implementing our comprehensive cybersecurity solutions, healthcare organizations can experience tangible benefits. They gain improved patient privacy, minimize the risk of data breaches, achieve enhanced compliance with privacy regulations, and streamline workflow efficiency.

We believe healthcare organizations can prioritize cybersecurity and take proactive measures to protect their valuable assets, but they don’t have to face this challenge alone. With Canon Medical’s expertise and cutting-edge solutions, healthcare organizations can rest easy, knowing they have the best possible protection to isolate their imaging equipment from cybersecurity threats both now and in the future.

Sources

1. Riggi, J. The importance of cybersecurity in protecting patient safety. AHA Center for Health and Innovation. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety
2. Healthcare Cybersecurity: The Biggest Stats and Trends in 2023. July 31, 2023 https://www.safetydetectives.com/blog/healthcare-cybersecurity-statistics/
3. Testimony of Erik Decker, Chairman, Cybersecurity Working Group of the Health Sector Coordinating Council and Vice President, Chief Information Security Officer, Intermountain Health on "Preparing for and Responding to Future Public Health Security Threats." May 11, 2023 (Page 2)
4. Gregory J. Increasingly Sophisticated Cyberattacks Target Healthcare. *Security Intelligence*. Published online June 1, 2023. Accessed June 16, 2023. https://securityintelligence.com/articles/increasingly-sophisticated-cyberattacks-target-healthcare/?c=Healthcare.
5. Greenberg A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *WIRED*. Published online August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
6. Alder S. Research Suggests Healthcare Data Breaches Cause 2,100 Deaths a Year. *The HIPAA JOURNAL*. Published online March 27, 2018 https://www.hipaajournal.com/research-suggests-healthcare-data-breaches-cause-2100-deaths-a-year/
7. Gregory J. What Has Changed Since the 2017 WannaCry Ransomware Attack? *Security Intelligence*. Published online September 1, 2021 https://securityintelligence.com/articles/what-has-changed-since-wannacry-ransomware-attack/
8. Donavan F. Orangeworm Jeopardizes Healthcare Data Security at Large Firms. *Health IT Security*. Published April 24, 2018. https://healthitsecurity.com/news/orangeworm-jeopardizes-healthcare-data-security-at-large-firms
9. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum*. 2022;3(12). doi:10.1001/jamahealthforum.2022.4873
10. Healthcare Data Breach Statistics https://www.hipaajournal.com/healthcare-data-breach-statistics/
11. Couture N, Decker E, Chua J, et al. A Case Study of "Cancer Care in the Wake of a Cyber Attack." HHS 405(d). October 2021. Accessed June 16, 2023. https://405d.hhs.gov/Documents/405d-spotlight-webinar-october2021.pdf.
12. Powell O. CommonSpirit Health reports that ransomware attack cost $160 million. *Cyber Security Hub*. Published June 2, 2023. https://www.cshub.com/attacks/news/commonspirit-health-reports-that-ransomware-attack-cost-160-million
13. Irwin L. List of Data Breaches and Cyber Attacks in 2023. *IT Governance*. Published August 1, 2023. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023
14. Burky A. Idaho hospital diverts ambulances, turns to paper charting following cyberattack. *Fierce Healthcare*. Published online June 1, 2023. Accessed June 16, 2023. https://www.fiercehealthcare.com/health-tech/over-24-hours-following-cyberattack-idaho-hospital-diverts-ambulances-turns-paper. Cost of a data breach 2022. IBM. Accessed June 16, 2023. https://www.ibm.com/reports/data-breach
15. 2022 Ransomware The True Cost to Business. https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf page 8
16. U.S. Securities and Exchange Commission. Press Release. SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/news/press-release/2023-139
17. H.R.2617 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2023. (2022, December 29). https://www.congress.gov/bill/117th-congress/house-bill/2617.
18. Center for Devices and Radiological Health. Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act. U.S. Food and Drug Administration. March 2023. https://www.fda.gov/media/166614/download

Canon

CANON MEDICAL SYSTEMS USA, INC.
https://us.medical.canon

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Disclaimer: Some features presented in this brochure may not be commercially available on all systems shown or may require the purchase of additional options. Please contact your local Canon Medical Systems representative for details.