Boston Scientific

Cybersecurity Assessment

04/16/2025

Team Members

Raneem Alarian, Ammar Shamsher, Tj Russell

Table of Contents

Company Profile

Boston Scientific is a global medical technology company founded in Marlborough, Massachusetts. The company aims at improving patient care by providing high-performance solutions and reducing the cost of healthcare for patients worldwide. The company specializes in designing and manufacturing minimally invasive medical devices used for diagnosing and treating various health conditions in fields such as cardiology, neurology, and urology. More specifically, Boston Scientific's medical devices focus on helping doctors perform procedures with smaller incisions, less pain, and quicker recovery times.

Boston Scientific is part of the medical device industry, which develops tools to diagnose and treat health conditions. This industry is vital to healthcare, offering everything from surgical instruments to advanced devices like pacemakers. It is fast moving, competitive, and driven by innovation. As the population ages and demand grows, companies like Boston Scientific lead in creating devices that improve patient care.

Overview

Boston Scientific's cybersecurity assessment recognizes the important assets that need to be protected from a variety of cybersecurity threats. The WATCHMAN FLX device is vulnerable to outdated software and remote attacks, which need to be secured through effective measures such as secure system configurations, regular backups, and incident response plans. Customer & Healthcare Professional Portals are vulnerable to malware infection and system downtime, and measures like data encryption, software patches, and incident response plans are required. The HeartLogic system is vulnerable to weak authentication and requires multi-factor authentication, role-based access controls, and regular security audits to secure patient information. Additionally, the Electronic Health Record (EHR) System is exposed to insider threats, which can be resolved through user activity monitoring and least privilege access controls. The use of AI and Machine Learning Algorithms is exposed to identity theft and privacy breaches, which can be minimized through enhanced data privacy controls and ethical AI. Patents & Trademarks also face risks, such as infringement and misuse, which can be mitigated by intellectual property monitoring and confidentiality agreements. Each of these assets requires specific controls to further Boston Scientific's cybersecurity position and protect sensitive patient information.

Asset Ranking

Company:	Boston Scientific			
Key Assets				
Digital Asset [1]	**Description**	**#**	**Value (1 - 10) [2]**	**Explanation/Reasoning**
WATCHMAN FLX™	This device is indicated to reduce the risk of stroke in patients with atrial fibrillation.		1	This is an important asset because it is crucial in the cardiovascular segment, the company's largest revenue generator. This ranks first because it is a flagship product that generates substantial revenue and directly impacts patient outcomes, making it one of the company's most vital and profitable assets.
LATITUDE™	LATITUDE™ is an online portal tailored to patients using specific devices. It provides essential health data, device performance tracking, and communication tools to help patients and healthcare providers manage care effectively.		2	This ranks second because the immediate impact on patient care and revenue generation makes it a critical asset. A cyberattack would expose sensitive patient information and compromise device performance, leading to financial and reputational harm. It is a crucial asset, but slightly less immediate in impact than the WATCHMAN FLX™ which more directly impacts patient safety in real-time.
Remote Patient Monitoring	By integrating medical devices with digital platforms, remote patient monitoring improves patient care by allowing for the continuous collection and transmission of patient data, such as vital signs or device performance, from a distance. It enables providers to monitor patients remotely, reducing the need for in-person visits.		3	This ranks third because RPM is critical for continuous patient monitoring, which means an attack could disrupt real-time data and patient care. While the impact is serious, it's less directly central to treatment than the devices themselves (like WATCHMAN FLX™ or LATITUDE™), so it ranks a bit lower.
Enterprise Risk Management Program	The Vice President of Global Internal Audit leads Boston Scientific's Enterprise Risk Management program (Boston Scientific, 2023). This program is designed to identify, assess, and mitigate any risks that could impact the company's operations, reputation, and financial performance.		4	This ranks fourth because the ERM program helps the company identify, prevent, and mitigate risks, including cyber threats. While a breach here could hamper response capabilities, it doesn't directly affect revenue or patient care, making it less critical than the actual medical devices or patient systems ranked above.
Global Security and Resiliency Experts	These professionals prepare for potential threats, including geopolitical, meteorologic, and climate-related events (Boston Scientific, 2023). They monitor the company's value chain with AI and visualization tools to ensure the company can withstand and recover from various disruptions that could impact their operations globally.		5	This ranks fifth because, although not tangible, these experts' efforts can help save millions of dollars in potential recovery costs, legal fees, and lost business. These experts are tasked with protecting the company's infrastructure from cyberattacks. If compromised, it would weaken the company's defenses, but the impact is indirect compared to losing patient-facing systems or core revenue-generating products.
BeatLogic™	BeatLogic is a cloud-based ECG analysis platform that uses AI algorithms and deep learning to support cardiologists and healthcare providers in making informed decisions for patients with atrial fibrillation.		6	This ranks sixth because while it's important for managing atrial fibrillation, a breach would affect a more niche group of patients. The impact would be limited compared to core systems like WATCHMAN FLX™, but it would still affect patient safety and the company's reputation.
Supply Chain and Operational Systems	Ensures the company can effectively manufacture, manage, and distribute its medical devices across the globe. These systems integrate a variety of technologies to improve efficiency, reduce costs, and enhance the timeliness and quality of the company's products.		7	Disrupting the supply chain would delay product manufacturing, impacting product availability and revenue. However, recovery options are more feasible than for patient care systems. It's still critical but ranked seventh because it doesn't immediately endanger patient safety.
Customer Service	Customer service provides technical support and addresses customer inquires. They ensure that healthcare providers and patients have the resources and information they need for the successful use of the company's products.		8	A cyberattack would primarily delay communication and response times. This ranks eighth because it doesn't immediately disrupt patient care or revenue generation, which makes it less critical than medical systems.
Trademarks	Trademarks ensure that Boston Scientific's products are easily recognized and distinguished from competitors. They protect the company's brand identity and reputation.		9	This ranks ninth because trademarks protect brand identity but don't directly affect revenue or patient care. A cyberattack would cause reputational harm, but it's less impactful than other core assets.
Research and Developmenet (R&D)	Boston Scientific heavily invests and funds in research and development to advance its portfolio of medical devices. This fuels new product development and enhances existing ones.		10	A cyberattack on R&D would delay future innovation and product rollouts, but it's a long-term risk rather than an immediate operational threat, which is why it ranks tenth.

Risk Management Matrix

Risk Management Matrix for Boston Scientific										
							RACI...			
#	Related Asset	Risk Description [1]	Business Consequences [2]	Severity (0 - 100) [3]	Likelihood (0 - 100%) [4]	Score (Severity * Likelihood) [5]	Mitigation [6]	Responsible	Accountable	Consulted
1	WATCHMAN FLX	Unauthorized access	Patient safety would be on the line, which in turn could cause reputational damage and legal consequences	95	45%	42.75	Encrypt patient data stored on the device, reguarly patch and update firmware/software, and conduct regular security audits	Information Technology	Executive Team	Legal
2	HeartLogic	Unauthorized access	Patient safety would be at risk, which could cause reputational damage and legal risks for the company	90	40%	36	Encrypt patient data, regularly update and patch firmware/software, and perform routine security audits	Information Technology	Executive Team	Legal
3	LithoVue	Device malfunction due to software vulnerabilites	This risk would impact patient safety and cause operational disruptions, reputational damage, and legal consequences	80	35%	28	Conduct regular software updates/patches and implement testing and validation & error recovery and redundancy	Information Technology	Executive Team	Legal
4	Device Firmware & Embedded Software	Malware	This risk would impact patient safety and cause financial consequences, reputational damage, and loss of intellectual property	95	65.00%	61.75	Implement strong authentication and access controls, regular firmware and software updates, implement anti-malware software, and use real-time monitoring and threat detection (IDS)	Information Technology	Executive Team	Operations
5	Cybersecurity & Data Protection Systems	Ransomware	This risk would impact operations, cause financial loss and reputational damage, and cause the exfiltration of sensitive data which could result in legal consequences and loss of trust from consumers	85	60.00%	51	Regular data backups, employee training and awareness, develop an incident response plan, and implement threat detection (IDS)	Information Technology	Executive Team	Operations
6	Electronic Health Record	Insider threats leaking sensitive data (intentionally and/or unintentionally)	This risk would result in HIPAA violations, loss of customer trust, financial losses from breach recovery, and reputational damage	65	50.00%	32.5	Use Role-Based Access Control, implement user activity and monitoring, use least privilege access, and conduct regular employee training	Information Technology	Executive Team	Legal
7	AI & Machine Learing Algorithms	Over-reliance on AI systems	Over-reliance could lead to incorrect AI decisions which could result in misdiagnosis or inappropriate treatments leading to legal liabilities, reputational damage, and loss of trust from healthcare professionals	60	30.00%	18	Implement Human-in-the-loop to help balance machine output with human judgment and use simulations and test environments to validate AI systems	Information Technology	Executive Team	Operations
8	Cloud & IT Infrastructure	Data breaches due to inadequate access controls	This risk could result in legal penalties, financial losses, and potential impact on future revenue due to damaged reputation and lost customer confidence	85	25.00%	21.25	Implement MFA, apply Role-Based Access Control, implement least privilege access principle, and conduct regular security audits and reviews	Information Technology	Executive Team	Operations
9	Patents & Trademarks	Unauthorized access	This risk could cause loss of intellectual property, loss of licensing revenue, and financial losses	70	20.00%	14	Implement MFA, use RBAC, enable access monitoring and auditing, and conduct regular security audits	Legal	Executive Team	Information Technology
10	Data Analytics & AI Platforms	Malware	This could cause disruption in production, financial losses, and operational disruption	75	60.00%	45	Implement anti-virus and anti-malware software, conduct regular software and firmware updates, use data encryption, and conduct regular backups and recovery plans	Information Technology	Executive Team	Operations
11	Customer & Healthcare Professional Portals	Data breaches	This risk could cause legal penalties, reputational damage, and loss of customer trust	90	65.00%	58.5	Encrypt data, implement MFA and RBAC, conduct regular security audits and vulnerability scanning, conduct regular user/employee training and awareness	Information Technology	Executive Team	Legal

Assessment Recommendations

WATCHMAN FLX and HeartLogic are the number two most important assets on the risk management matrix based on their high business criticality in both patient care and business operations. If they are compromised, patient safety would be on the line which would cause legal consequences and reputational damage to the company. The EHR system and AI & Machine Learning assets rank in the middle but remain vital to the business, as their compromise would cause interruptions of operations, monetary losses, and reputational consequences. Patents & Trademarks and the Customer & Healthcare Professional Portals are also important, even though they pose less immediate threat, they too need protection to make sure the company maintains its competitive position and safeguards customer data. Their compromise would result in legal penalties, financial loss, and reputational damage.

For **WATCHMAN FLX,** encryption and frequent backups are essential in safeguarding patient data from system breakdown and cyberattack. In this way, data will remain accessible and secure even in case of an attack. Unauthorized access is restricted by multi-factor authentication (MFA), while security updates and scans identify and repair vulnerabilities before they can become an issue. For **Customer & Healthcare Portals**, encryption is used to protect sensitive data in transit and at rest. Encryption ensures that even if data is intercepted, it will be illegible. An incident response plan enables rapid response in case of breaches, and routine audits ensure compliance with privacy regulations, maintaining trust and security. For **HeartLogic**, Multi-Factor Authentication (MFA) ensures that sensitive patient information is accessed only by authorized individuals, reducing the risk of unauthorized access. Ongoing monitoring logs system activity, identifying any suspicious behavior in real-time. For **Electronic Health Records (EHR)**, least-privilege access limits each user's access to just the data that's necessary for their job role, reducing the harm caused by insider threats. Regular auditing and review unveil any control access issues so that sensitive data remains protected. For **AI & Machine Learning**, encryption and anonymization techniques prevent unauthorized access to personal data, maintaining privacy and security. Real-time monitoring watches AI behavior and warns of suspicious activity or potential breaches. Regular algorithm audits uncover biases, ensuring fair and secure outcomes, and MFA prevents impersonation and spoofing access. For **Trademarks & Patents,** active IP management, through the use of automated tools, enables early detection of potential infringements with minimal risk of loss of assets. Periodic IP audits guarantee that patents and trademarks are well protected, maintained, and enforced.

WATCHMAN FLX (Ammar Shamsher)

The WATCHMAN FLX is a small heart implant that helps reduce the risk of stroke in patients that have heart problems also known as AFib. This device closes off parts of the heart where blood clots can form. A major risk of this is **Remote Exploits and Outdated Software**. Many hospitals still use outdated systems such as Windows 7 or even older, which no longer receive important security updates making it an easy target for cyber attackers. These attackers can take advantage of the known flaw in these outdated systems to gain access without much effort. If the attacker breaks into an imaging system during a WATCHMAN FLX procedure, they could change or distort the images the doctors rely on, making it harder to see the heart clearly. The system might crash or stop working entirely in the middle of the procedure, leading to delays harming the patient if the doctor can't properly guide the implant.

The risk function/category/sub-category

It is important to recognize that the WATCHMAN FLX stores data for the doctor and patient to examine and there has to be proper protection implaced for it. That is why it would fall under the **Protect (PR)** risk function, within the **Information Protection Processes and Procedures (PR.IP)** category. Although the WATCHMAN FLX implant doesn't use the internet or store any data, the steps taken before, during and after the procedure such as "preparing the patient, taking heart images, handling medical records, and doing check-ups all involve important and private information" (Watchman FLXTM, 2019). The Information Protection Processes and Procedures (PR.IP) category is about making sure hospitals have clear and reliable rules in place to keep that information safe. This fits well with the WATCHMAN FLX because it helps protect the systems and tools used during the procedure from cyber risks, even though the implant itself isn't digital. A sub-category related to WATCHMAN and PR.IP is **Backups of Information are Conducted, Maintained, and Tested (PR.IP-4)**. Patient records, imaging data, and procedure documentation related to WATCHMAN FLX should be backed up regularly in case of system failures or cyberattacks.

Policy and Procedures

Setting up System Safety is most important for the WATCHMAN FLX and should be followed. These systems handle important patient data and support the device's function, so **security and privacy are top priorities**. Only trained and approved staff should be allowed to access or set up these systems. All employees must use secure logins, and access should be

limited based on job roles. Patient information must always be protected through **encryption**, both when it's stored and when it's being sent. Any changes made to the system should be recorded in logs and reviewed regularly for any signs of unusual activity.

When setting up a system, it's important to first check that the hardware and software are compatible with the WATCHMAN FLX and have passed safety checks. Before connecting the system to the network, all software updates should be installed. Default settings and passwords should be changed, and unused features or services should be turned off to reduce risks. Security tools like antivirus software should be installed, and the system's hard drive should be encrypted to protect data.

Recommended Control

To ensure that systems supporting the WATCHMAN FLX device are set up safely and securely, a thorough validation process must be followed. Before the system is used in a real environment, a full security review should be completed. This includes running vulnerability scans to check for any weaknesses, confirming that the latest software updates and security patches have been installed, and reviewing user access to make sure only authorized staff can log in. "**Strong passwords** should be in place, and **multi-factor authentication (MFA)** must be enabled to provide an extra layer of security. Before the system goes live, a final checklist should be reviewed and approved by a qualified member of the **IT security** team or another responsible party" (Walker, 2023).

Customer & Healthcare Professional Portals (Ammar Shamsher)

These online platforms allow doctors, hospitals, and customers to find product information, training, and support services. The portals have many different risks that could potentially occur. One being **Malware Infiltration**, this happens when harmful software snacks into a system. If Boston Scientific's customer or healthcare professional portals have security weaknesses such as outdated software, unprotected file uploads, or unsecured form fields cyberattackers might use these to install malware. This could include spyware which secretly monitors users. Ransomware which locks the system and demands money or other harmful programs. Once inside, malware could steal login details, patient data, or even damage the system. It can also spread to other parts of the network, affecting more systems and putting even more information at risk. Even one small flaw in the portal could be enough for malware to get in and cause serious problems. Another risk being **System Downtime**, this happens when the portal becomes slow or stops working. A common cause is DDoS attack, where cyberattackers

flood the site with traffic to make it crash. These attacks don't steal data but can block access for healthcare professionals and customers. This can delay care, disrupt support services, and damage trust even without a data breach.

The risk function/category/sub-category

As it can be seen, customer and healthcare portals have many risks that could possibly occur. That is why the portals would fall under **Respond (RS)** risk function, within the **Analysis (RS.AN)** category. This focuses on carefully examining a cybersecurity incident after it has been found. This is a very important step, especially for systems like Boston Scientific's Customer and Healthcare Professional Portals, which deal with sensitive information such as patient records and healthcare provider details. When something goes wrong like a malware infection, phishing attack, DDoS disruption, or someone gaining access without permission the company needs to quickly investigate what happened. This means understanding who was affected, what kind of information was at risk, how the attack happened, and whether the threat is still active. A sub-category related to the portals and RS.AN is **Response Roles and Responsibilities are Assigned (RS.CO-1)** this is about making sure that everyone knows what their role is and what they need to do during a cybersecurity incident. For example, if something goes wrong with Boston Scientific's customer or healthcare portals like a data breach or system outage there should already be a clear plan in place that says who is responsible for what. The IT team might work on fixing the technical issue, the security team might investigate how the incident happened, the legal team might review what laws apply, and the communications team might inform customers or healthcare professionals if needed.

Policy and Procedures

To protect sensitive information in Customer and Healthcare Professional Portals, strong **data encryption** must be used. This includes data being sent over the internet and data stored in systems. All information shared through the portals such as medical history, personal details, and login information should be encrypted using secure methods. For instance, "websites should use **HTTPS to keep data safe while it travels**, and data stored in files or databases should be protected with strong encryption and **AES-256**" (Kanand, 2024). This helps make sure that even if a cyberattacker tries to access the data without permission, they won't be able to read it.

All staff using or managing these portals should be trained on how to handle encrypted data and report any security concerns. Regular checks, such as "security scans and audits, should be done to make sure encryption is working properly and that the system meets privacy laws like

HIPAA or GDPR" (Calderon, 2023). By following these steps, healthcare organizations can keep patient data safe, build trust, and reduce the risk of data breaches.

Recommended Control

To confirm that data encryption is working correctly, **regular security checks should be performed.** This includes verifying that all personal and medical data remains protected both during transmission and while stored in systems. **Reviews should ensure that up-to-date encryption protocols and secure transport methods are in place.** Encryption keys must be safely managed, with limited access and routine rotation.

HeartLogic (Raneem Alarian)

HeartLogic is a heart failure monitoring device utilized to keep track of patients with heart failure. It belongs to the Cardiac Rhythm Management (CRM) family and is designed to detect early evidence of worsening heart failure symptoms through continuous monitoring of a patient's heart function as well as other physiological parameters. This system receives data from implanted devices such as pacemakers or defibrillators to track a variety of parameters including heart rate, respiration, thoracic impedance, and physical activity levels. The data is then transmitted to healthcare providers for interpretation and intervention. Although a competitive edge for Boston Scientific, there are **risks** associated with the asset, such as **weak authentication leading to stolen sensitive information**. If the authentication process does not enforce strong authentication measures, then attackers can gain access to the system. Once they've gained access, they are capable of altering patient information, modifying device settings, or even disabling critical monitoring functions, which would have direct implications for patient safety. Moreover, weak authentication gives the attackers an easier entry point to the network from which data is being transmitted, and hence they are capable of intercepting or tampering with the sensitive information being delivered to healthcare providers.

The risk function/category/sub-category

HeartLogic falls under the **Identify (ID) Risk Function** because this function focuses on understanding and managing access to systems and data. In this case, **the risk involves weak authentication**, which directly ties into how identities are managed and access is granted. This asset falls under the **category** of **Asset Management (ID.AM)** because this category is responsible for making sure that organizations identify and authenticate people and devices before giving them access to the systems and data (CSF Tools, n.d.). In terms of sub-category,

this asset falls under the sub-category **ID.AM-2: Software platforms and applications within the organization are inventoried.** For HeartLogic, this means having confidence that software employed to monitor and manage patients' heart conditions and any devices it is interfaced with, like pacemakers or defibrillators, is inventoried and secured.

Policy and Procedures

To offset the possibility of weak authentication leading to unauthorized access in the HeartLogic system, the company will **enforce Multi-Factor Authentication (MFA)** to all users of the HeartLogic system to help safeguard sensitive patient data. The policy will be used to properly authenticate each individual using a minimum of two modes of verification before accessing the system. This policy avoids or at least reduces unauthorized access, which can be created by weak or compromised passwords, and adds an extra layer of protection to the system (Georgia Technology Authority, n.d.).

To implement the Multi-Factor Authentication (MFA) policy, **the company will first install the HeartLogic system to apply MFA to all the users** accessing sensitive data or system functions. Such users include healthcare providers, administrators, and all staff that engage with important patient information. The procedure will be to make sure that **users authenticate with their password and a one-time passcode sent to their mobile device.** All the users will be required to sign up for MFA upon their initial login, and training will be provided on the installation and use of MFA.

Recommended Control

In order to ensure that the Multi-Factor Authentication (MFA) policy is running successfully, the company will employ **an automated monitoring system that tracks and logs all MFA authentication requests**. The system will notify on any failed MFA attempts and generate real-time reports to identify any issues with authentication, such as repeated failed logins or bypassed MFA requirements. The company will also **conduct quarterly audits** to ensure that all the users are enrolled properly in MFA and are applying the appropriate authentication processes. The audits will monitor system access logs and ensure that all users are required to use MFA prior to accessing sensitive data. The efficiency of MFA will **further be attested by examining incident response reports** to verify any security incidents related to MFA, such as attempted breaches or unauthorized access, are properly investigated and mitigated. Not only does this multi-control system enforce the MFA policy, but it also actively protects the HeartLogic system from unauthorized access.

Electronic Health Record System (Raneem Alarian)

Boston Scientific's **Electronic Health Record System** is a valuable asset containing sensitive patient data, including medical histories, diagnoses, treatment, and other personal health information. The system is widely used by healthcare providers to coordinate care and ensure treatment continuity. But the **risk of insider threat** comes about when the organization's members, such as employees, contractors, or other authorized people, misuse their access to the EHR system unintentionally or with intent. These insiders can steal sensitive data, modify patient records, or cause disruption, either for financial gains or for malicious purposes, leading to significant privacy breaches, regulatory violations, and company reputation loss.

The risk function/category/sub-category

Since the risk of insider threat is focused on detecting unusual or unauthorized activity within the **EHR System**, the appropriate **Risk Function is Detect**. The function highlights the importance of potential security breaches being detected at the earliest opportunity so that organizations are adequately prepared to respond in the right way to threats. The **Detect function** makes sure that malicious activity, including insider activity, is identified and countered in a timely manner to prevent damage. For the **category**, the most relevant one would be **Anomalies and Events (DE.AE): Anomalous activity is detected,** as it focuses on detecting anomalies in system activity or user behavior that might indicate a security incident (National Institute of Standards and Technology [NIST], n.d.). Insider attacks typically present themselves as unusual access patterns, unauthorized record changes, or efforts to exfiltrate sensitive data (Teramind, 2025). This asset would fall under the associated **sub-category DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.** This sub-category emphasizes the necessity of tracking personnel activity closely to detect any atypical or malicious activity. Through tracking personnel activity, organizations are able to detect possible insider threats in advance and rectify them before sensitive data are compromised or altered.

Policy and Procedures

To minimize the risk of insider threats to Boston Scientific's Electronic Health Record (EHR) System, the company will **implement a strategy of continuous user activity monitoring in combination with least-privilege access controls**. The policy mandates that all user activity within the EHR system must be logged and actively monitored for any sign of

anomalous activity. In addition, only the minimum privileges necessary will be assigned to employees and based on their specific job function (Edwardson, 2025).

To enforce the policy, **the company will integrate a user activity logging system into the EHR System platform** to continuously track all user activity, such as logins, data access, changes, and exports. The logs will be securely stored and monitored in real-time, with automated alerts set up to identify suspicious activity. Moreover, **least-privilege access controls shall also be applied by the company** by ensuring the users only receive access to that data needed based on their designation.

Recommended Control

To verify that the policy is working properly, **the security team will continually review the activity logging system reports** to make sure that it is accurately capturing user activities and detecting unusual behavior. Furthermore, **quarterly access reviews will be conducted by the company**, wherein IT and HR will verify that workers have only the access levels they need to perform their job function, and that least-privilege access controls are enforced. Any circumvention of the expected levels of access will be addressed on a timely basis. **Regular system audits** will also be conducted to confirm that the logging system is functioning as should be expected, and that any gaps in access control will be addressed.

AI & Machine Learning Algorithms (Tj Russell)

AI (Artificial Intelligence) and machine learning (ML) algorithms are computational systems designed to mimic human intelligence and learn from data. AI is the umbrella term for a wide range of technologies that enable machines to carry out activities like pattern recognition, decision-making, and problem-solving. Developing models that can learn from and get better based on data without explicit programming is the goal of machine learning, a branch of artificial intelligence. **These algorithms examine huge datasets in order to find trends, forecast outcomes, or automate procedures**. As the models receive more data, they improve their predictions or actions over time, allowing for ongoing development and adaptation across a range of applications, including predictive analytics, image recognition, and language processing.

The risk function/category/sub-category

Since **AI and machine learning algorithms** frequently depend on enormous volumes of personal data to operate, they a**re susceptible to identity theft, data breaches, and privacy**

violations. This puts them within the category of **Identity(ID), within Asset Management(ID.AM)**. These systems may unintentionally reveal or misuse personal information as they use sensitive data to predict actions or make judgments, particularly if appropriate security and privacy safeguards aren't in place. Furthermore, discriminatory results might arise from biased algorithms that adversely affect people based on personal traits like gender, race, or economic status. Furthermore, "people are vulnerable to manipulation and **impersonation due to the potential for identity fraud using AI technologies like deepfakes and face recognition** (Chesney & Citron, 2019; Westerlund, 2019)".

Policy and Procedures

Organizations utilizing AI and machine learning technologies must prioritize the protection of personal data by implementing comprehensive privacy measures. "This includes **data encryption, anonymization, and secure access** management to prevent unauthorized access and exposure of sensitive information (Shokri et al., 2017)". Advanced privacy techniques such as differential privacy should be employed to safeguard individual identities while still enabling valuable insights from large datasets. Regular assessments of algorithms for fairness, transparency, and bias must be conducted to prevent discriminatory outcomes and ensure that decision-making processes remain equitable. All AI systems must comply with data protection regulations, including **GDPR**, to protect personal information and maintain public trust.

To secure AI and machine learning systems, organizations must establish clear procedures for monitoring and mitigating security risks. **Strong identity verification mechanisms, including multi-factor authentication (MFA)**, should be implemented to reduce the risk of impersonation or fraud. Continuous monitoring of AI systems is essential to detect any unusual activity or security breaches, with prompt action taken to address any vulnerabilities. Additionally, organizations must r**egularly audit AI models** to assess their accuracy and detect any potential biases that could lead to discriminatory or harmful outcomes. These security measures should be aligned with industry best practices and compliance requirements to safeguard personal data and ensure the integrity of AI-driven processes.

Recommended Control

Organizations should have strong privacy and security measures in place, like **data anonymization, encryption, and access management, to reduce the risks connected to AI and machine learning systems.** By using cutting-edge strategies like differential privacy, sensitive personal information can be protected while yet allowing for insightful analysis of big datasets. To avoid discriminatory results, it is **also essential to routinely assess algorithms for**

fairness, openness, and bias. Strong identity verification procedures must be put in place to lower the possibility of manipulation and impersonation, and ongoing monitoring is necessary to spot any odd activity or any security breaches. Last but not least, putting **multi-factor authentication (MFA)** into place and making sure that data protection laws like the GDPR are followed can help protect private data from abuse and illegal access.

Patents & Trademarks (Tj Russell)

Trademarks and patents are types of intellectual property protection that give businesses and creators exclusive rights. A patent prevents new innovations or processes from being copied by granting the owner the sole right to produce, use, or market the invention for a predetermined amount of time, usually 20 years. **Conversely, a trademark is a word, phrase, symbol, or logo that sets one company's products or services apart from another** and provides the brand identity with legal protection. Trademarks protect consumer trust and brand recognition, allowing firms to maintain a distinct position in the market, whereas patents concentrate on protecting novel items or technologies. “Both are essential instruments for safeguarding commercial interests, creativity, and innovation (Maskus, 2000)”.

The risk function/category/sub-category

Patents and trademarks can fall under the **"Recover" risk function** within **Recovery Planning(RC.RP)** because the process of protecting and enforcing these intellectual property (IP) rights can be costly, time-consuming, and challenging, especially if infringement or disputes arise. “The legal fights necessary to claim ownership or recover damages in the event of a patent or trademark infringement can be costly and cause a delay in recovering lost earnings (Lerner, 2006)”. Additionally, a business runs the danger of losing its exclusive rights or compromising the security of its assets if it neglects to adequately monitor or enforce its **intellectual property**. Furthermore, the IP holder can lose their ability to recover their investment or lessen financial losses if a patent or trademark is declared invalid or successfully challenged, which could weaken their position as a market leader.

Policy and Procedures

To properly protect patents and trademarks, organizations need to put in place a thorough **intellectual property (IP) management policy**. This involves a proactive approach to IP rights monitoring and enforcement, with automated tools and IP surveillance services being used on a regular basis to look for possible infringements. To guarantee that patents and trademarks are

appropriately **registered, documented, and protected against any challenges**, the company should make an investment in capable legal counsel. Businesses should also adopt clear policies for safeguarding intellectual property, making sure that all patents and trademarks are upheld and enforced in compliance with the law. Companies must also train staff members on the value of intellectual property protection and the consequences of ignoring it in order to preserve customer confidence and the company's place in the market.

Businesses should build up processes for routine **IP audits** to evaluate the security and robustness of their intellectual property assets in order to enforce the protection of patents and trademarks. This involves collaborating with legal professionals, including intellectual **property advisors or patent attorneys**, to quickly resolve any possible disagreements or infringement concerns. Companies should keep a close eye on the market to spot instances of unapproved use of their trademarks or patents, and if needed, take prompt legal action to protect their exclusive rights. Additionally, companies should keep up good contacts with outside partners to enable prompt dispute resolution. To keep up with the evolving legal and commercial landscape, these protocols need to be evaluated and modified on a regular basis.

Recommended Control

Organizations should **put in place a proactive intellectual property (IP) management plan** to avoid the risks related to the defense and enforcement of patents and trademarks. In order to identify unlawful usage of patents or trademarks early on, this involves **routinely checking for possible infringements using automated tools and IP surveillance services.** In order to resolve conflicts effectively and guarantee that their intellectual property rights are appropriately registered, recorded, and upheld, businesses should **also make significant investments in strong legal counsel.** Furthermore, **developing solid bonds with other partners** like patent lawyers or intellectual property consultants can facilitate navigating intricate legal systems and quickly resolving possible issues. The continued security and value of patents and trademarks can also be guaranteed by carrying out recurring IP audits and training staff members on the significance of protecting intellectual assets.

Conclusion

In conclusion the assets WATCHMAN FLX, HeartLogic, Electronic Health Record (EHR) system, AI & Machine Learning algorithms, Patents & Trademarks, and Customer & Healthcare Professional Portals are some of the most important parts of Boston Scientific work. These assets handle sensitive data, protect patient safety, and help the company stay ahead in the medical field. If any of these assets were compromised, it could cause serious problems like data breach, patient harm, legal trouble, or damage to the company's reputations.

Each policy, procedure, and controle suggested in this assessment is designed to fix the specific risks these assets face. For example, the WATCHMAN FLX device is at risk of remote attacks and outdated software. This is why it requires strong system settings, secure backups, and a clear response plan if something goes wrong. The Customer and Healthcare Portals also need strong protections because they connect directly with external users. If these portals are attacked or infected with malware, it could lead to stolen personal data, system downtime, and lost trust. Using data encryption, applying security patches on time, and having a well developed response plan can greatly reduce these risks and help services stay up and running.

The HeartLogic monitoring system collects important patient data, so it needs strong protection. Using multi factor authentication, giving users only the access they need, and doing regular security checks can help prevent unauthorized access. For the EHR system, the biggest risk comes from inside the organization. That is why it is important to monitor user activity and limit access, making sure employees only see the data they need for their jobs. The AI and Machine Learning tools also carry risks, like identity theft and privacy issues. Adding better privacy settings and following ethical guidelines helps protect patient data and makes sure the systems work fairly. Finally, the company's Patents and Trademarks are key to keeping its competitive edge. Protecting these with monitoring, legal tools, and confidentiality agreements helps prevent them from being stolen or misused.

Altogether, the policies, procedures, and controls that are recommended will help Boston Scientific strengthen its cybersecurity framework. By targeting the specific risks each asset faces, the company can reduce the chances of attacks, follow healthcare and privacy regulations, and protect both patients and business operations. Taking a strong and well thought out approach to cybersecurity not only keeps the company safe but also builds trust with consumers, healthcare providers, and investors. It shows that Boston Scientific is fully committed to protecting its systems, its data, and the people who rely on its products in today's fast changing digital world.

References

Asset management - CSF tools. CSF Tools - The Cybersecurity Framework for Humans. (2021). https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-am/

Calderon, N. (2023, November 17). Hipaa vs GDPR compliance: A comprehensive comparison. MedStack. https://medstack.co/blog/hipaa-vs-gdpr/

Chesney, R., & Citron, D. K. (2019). "Deepfakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review*, 107(5), 1753-1819.https://www.law.virginia.edu/scholarship/publication/danielle-k-citron/1151906

Detect. NIST. (2018, May 21). https://www.nist.gov/cyberframework/detect

Edwardson, R. D. (2025, March 3). Implementing continuous monitoring and least privilege audits for Enhanced Security. Medium. https://medium.com/o-m-n-i-navigating-the-new-cyber-era/implementing-continuous-monitoring-and-least-privilege-audits-for-enhanced-security-0970c95c24c0

Lerner, J. (2006). *The Litigation of Patent Infringement*. Journal of Law and Economics, 49(1), 109-130.https://www.journals.uchicago.edu/doi/10.1086/655757#

Maskus, K. E. (2000). *Intellectual Property Rights in the Global Economy*. Institute for International Economics.https://cup.columbia.edu/book/intellectual-property-rights-in-the-global-economy/9780881322828/

Multi-factor authentication policy (PS-21-002) (n.d.). Enterprise Policies, Standards, andGuidelines. https://gta-psg.georgia.gov/psg/multi-factor-authentication-policy-ps-21-002

Shokri, R., Stronati, M., Song, L., & Shmatikov, V. (2017). "Membership Inference Attacks Against Machine Learning Models." *Proceedings of the 2017 IEEE Symposium on Security and Privacy*, 3-18.https://ieeexplore.ieee.org/document/7958568

Walker, J. (2023, October 2). Strong password best practices and MFA. Fortinet Blog. https://www.fortinet.com/blog/industry-trends/strong-password-best-practices-and-mf

Watchman FLXTM. www.bostonscientific.com. (2019, February 1).

https://www.bostonscientific.com/en-US/products/laac-system/watchman-flx.html

What is an insider threat? (2025). Teramind Blog. https://www.teramind.co/blog/insider-threats/#:~:text=Insider%20threats%20often%20l