<

Johnson & Johnson

Cybersecurity Assessment

2/11/2026

Harold Vernon

<

<

Table of Contents

Johnson & Johnson
Cybersecurity Assessment Report

Johnson & Johnson Profile

Information from the company website and other readily available content. Must include an image of a recent stock chart.

Company Description

Johnson & Johnson is a pharmaceutical company headquartered in New Brunswick, New Jersey. As of February 11, 2026, the company employs 138,000 people and hosts sixty-four manufacturing facilities worldwide according to its website. It is segmented into two parts, Innovative Medicine and MedTech. This segmentation provides both breadth and specificity to the services it provides by allowing the two segments to independently focus on different operations.

Company History

Johnson & Johnson was founded in 1886 by Robert Wood Johnson and his two younger brothers. This was ten years after Johnson attended the Centennial Exposition in Pennsylvania where he was first introduced to the concept of sterile surgery, which is what inspired him to start a business mass-producing antiseptic surgical supplies. From just fourteen employees in 1886, Johnson & Johnson grew to employ four hundred people by 1894. The company's primary niche was providing clean cotton to hospitals, which gave it an edge over most of its competitors which provided cotton filled with dirt and plant materials. This cotton was supplied in sheets that could be cut to fit the size of a wound, making surgery significantly safer than it had been previously by reducing the risk of sepsis.

From this first niche, Johnson & Johnson would expand throughout the 1880s and 1890s to provide other methods of preventing sepsis. These ranged from artificial sponges to steam machines to sterilize equipment. 1897 saw the expansion of Johnson & Johnson's laboratories to spearhead research and development (R&D.) Johnson & Johnson became a publicly traded company in 1944, shifting away from absolute executive leadership. This move provided the funds needed to expand R&D and international operations. In the 1960s, Johnson & Johnson segmented into Innovative Medicine and MedTech.

About the industry

The primary focus of Johnson & Johnson as of 2026 is research and development. Through the Innovative Medicine segment, Johnson & Johnson focuses on research into oncology, immunology, neuroscience, and cardiopulmonary medicine. Meanwhile through MedTech,

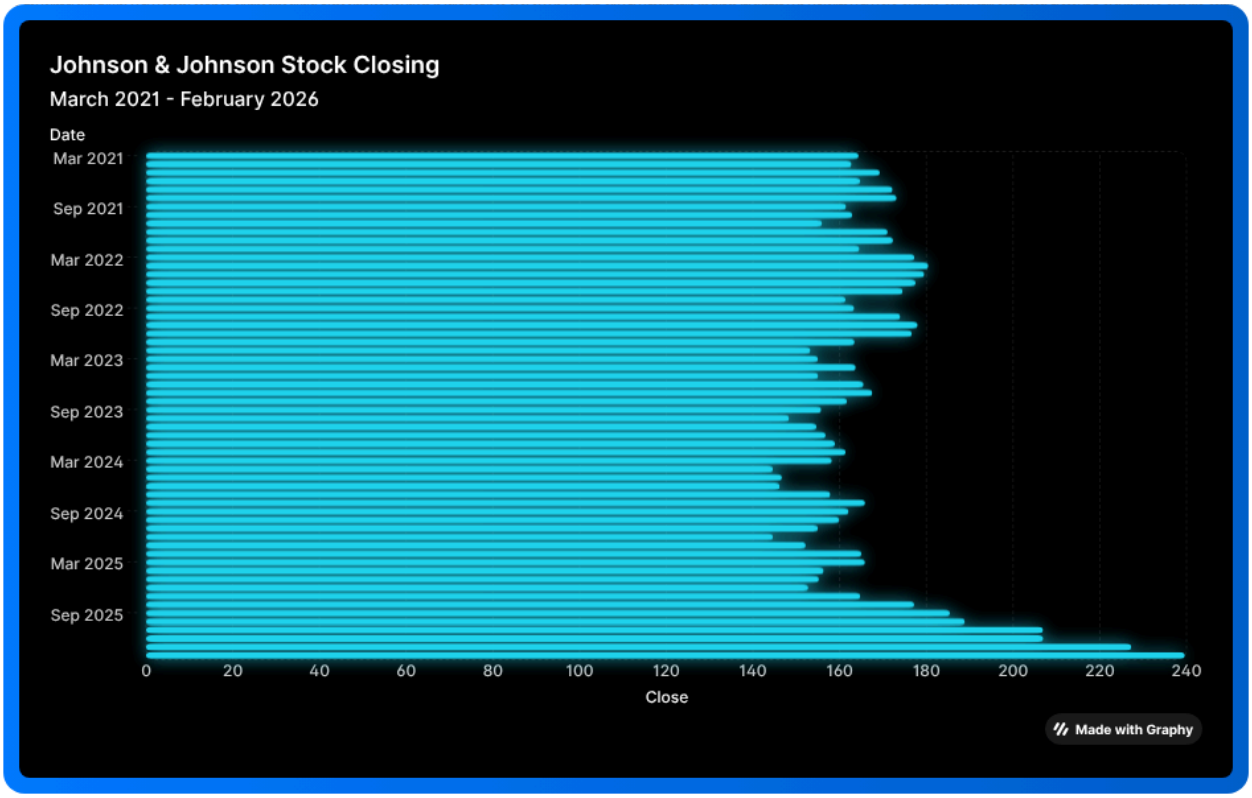
Johnson & Johnson
Cybersecurity Assessment Report

Johnson & Johnson focuses on the implementation of new technologies in medical settings. Special attention is paid by MedTech to cardiovascular, orthopedic, and optical operations, with a general focus on surgery as well. This focus, as well as the company's robust humanitarian efforts, gives Johnson & Johnson a greater degree of authority in the medical industry compared to its competitors.

Key Products

Intravascular lithotripsy (IVL) is a product developed by Shockwave, a subsidiary of Johnson & Johnson. It uses ultrasonic acoustic pressure waves to break up calcified plaque in the coronary arteries. This unique system is noted as being minimally invasive compared to other methods of breaking up potentially life-threatening arterial plaque. The shockwaves created by IVL leave healthy tissue unharmed while cracking calcified buildup. This is due to the similar density of the tissue and the saline being used to transmit the shockwaves. With the buildup weakened, medical professionals then use a balloon catheter to restore blood flow through the artery.

Stock Performance



Johnson & Johnson
Cybersecurity Assessment Report

Bottom Line Up Front (BLUF)

From the perspective of an executive at Johnson & Johnson, the main cybersecurity risk would be in products sold to healthcare providers that can connect to Johnson & Johnson networks. This is because said healthcare providers may have significantly more lax cybersecurity policies than Johnson & Johnson itself. Therefore, devices under their network that can still connect to Johnson & Johnson's networks are at risk of being used by malicious actors as a starting point for an attack against Johnson & Johnson that company cybersecurity teams are near-powerless to prevent. Legal teams, however, can prevent this by demanding that clients comply with cybersecurity regulations and best practices.

Interaction with outside systems is the overall theme of the cybersecurity threats facing Johnson & Johnson. While the company does have a fairly robust cybersecurity policy and infrastructure, it cannot be guaranteed that clients and partners will have similar approaches. Maintaining security while interacting with third parties then should be a focus of Johnson & Johnson's cybersecurity efforts. This can be done by enforcing compliance with cybersecurity standards as previously mentioned, but also by building security tools into products shipped out by Johnson & Johnson. An example of this in action would be shipping out Johnson & Johnson products with already robust encryption algorithms for the data they import, store, and export. However this might slow the speed at which data is transferred, which can be a serious problem in a medical setting that relies on precisely timed data measurements to both gather information on a patient and carry out treatments. This means that a balance must be found between security and efficiency

when it comes to the encryption that would hypothetically be built into Johnson & Johnson products that import, store, and export data.

In addition to building cybersecurity tools into their products, Johnson & Johnson can also help build up cybersecurity defenses within the medical industry broadly. This can take the form of educating clients and other third parties on cybersecurity best practices. While forcing third parties to comply with Johnson & Johnson's in-house policies would be controversial, impractical, and limit the company's pool of future partners, what can be done is work with both clients and competitors to establish a singular cybersecurity framework tailored to the healthcare industry. This is a far better choice than attempting to enforce Johnson & Johnson's policies universally because establishing a shared framework signals compromise and can be carried out in a way that meets the basic needs of all the organizations that agree to it, with more specific policies being left to individual organizations to craft as they see fit. This might be needed if the differing laws of nations that companies agreeing to this framework operate within require certain actions regarding consumer privacy and the safe storage of data, which is a particular concern if Johnson & Johnson's partners are based out of a country in the EU, which enforces one of the most robust sets of privacy regulations in the world.

While improving how Johnson & Johnson interacts with third parties, the company's own cybersecurity should not fall aside. Johnson & Johnson then needs to make sure that its cybersecurity teams remain up-to-date on present threats that might impact operations or data. This includes not just information released by journals and news sources, but also regular auditing of internal compliance with cybersecurity standards.

Johnson & Johnson
Cybersecurity Assessment Report

To conclude, Johnson & Johnson's main concern in cybersecurity terms is the fact that third parties will oftentimes have significantly different cybersecurity policies than Johnson & Johnson itself which may at times be less strict and thus easier for threat actors to exploit. This can be remedied by coordinating a shared cybersecurity framework within the healthcare industry and shipping out products with prebuilt security measures. While doing this, Johnson & Johnson must also avoid becoming complacent in regard to in-house cybersecurity.

Asset Ranking

Using the Risk Management Matrix, identify 10 assets you've identified and rank them in terms of importance. You will then select four of these assets (below) to provide recommendations.

Risk Management Matrix

Assessment Recommendations

A brief overview of your rationale for choosing your selected four (of the ten above) assets, risks to those assets, and recommended mitigation.

Asset 1

Asset:	Website
Risk:	SQL Poisoning
Function:	Protect
Category:	Data Security (PR.PS)
Sub-Category:	Software is maintained, replaced, and removed commensurate with risk (PR.PS-02)

Johnson & Johnson
Cybersecurity Assessment Report

Rationale	
This is your reasoning for selecting this Category/Sub-Category. A paragraph explaining your logic is sufficient.	
Policy:	The website must be protected from the threat of unwanted code being executed through SQL poisoning.
Procedure:	Input sanitization is a way to prevent most low-level threat actors from successfully conducting SQL poisoning operations. Input validation is another way to protect the website from attacks by low-skill and unprofessional threat actors. Implementing parameterized queries is a more difficult barrier for attackers to cross, useful if the threat is from professional hackers - which is probably for a large corporation such as Johnson & Johnson. Staying up-to-date on database software updates is a general best practice both for SQL poisoning and for overall security and efficiency.
Review Period:	The review period would consist of about five days at the beginning of each month to test security protocols employed to prevent SQL poisoning.
Control:	Red Teaming exercises would be employed to test the protocols used against SQL poisoning. These exercises would be conducted by the best cybersecurity professionals in the company to ensure that all reasonable threats are detected for future countering. Absolute thoroughness is to be employed by the red team to catch oversights before threat actors do. Exercises will be conducted in a cloned environment of the real Johnson & Johnson website to ensure that the red team can find every possible exploit without causing real damage to Johnson & Johnson's website. If the red team cannot get through despite their best efforts, then SQL poisoning is sufficiently protected against for that month. Though active monitoring protocols should still be maintained.

Asset 2

Asset:	Headquarters
Risk:	Weather Damage

Johnson & Johnson
Cybersecurity Assessment Report

Function:	Protect
Category:	Technology Infrastructure Resilience (PR.IR)
Sub-Category:	The organization's technology assets are protected from environmental threats (PR.IR-02)
Rationale This is your reasoning for selecting this Category/Sub-Category. A paragraph explaining your logic is sufficient.	
Policy:	The headquarters must be resilient against weather damage and business operations must be able to continue if damage occurs.
Procedure:	Frequent reviews of the headquarters' architecture to ensure resilience against the environmental threats facing New Jersey such as snowstorms and rare but potentially devastating hurricanes. Backup generators within the headquarters to provide power to critical systems in the event of an outage. General practice of backing up important data to a preferably in-house cloud server so that environmental damages occurring at a particularly unfortunate time do not mean the loss of valuable data that would be difficult to reproduce.
Review Period:	One week out of each year to inspect physical buildings. Daily backups of main servers.
Control:	Annual inspections will be carried out to ensure that buildings are compliant with local government regulations and safety codes. In addition, inspections will be carried out to see if buildings are compliant with in-house standards. The data critical to Johnson & Johnson's operations will be backed up to an in-house cloud server daily. This approach both diminishes the likelihood of weather damage disrupting operations and provides redundancy so that operations can continue in some limited form in the event that weather damages physical buildings and network devices.

Johnson & Johnson
Cybersecurity Assessment Report

Conclusion

The subcategories for how to protect the two assets in question (headquarters and website) from the most immediate risks identified - those being SQL Poisoning and weather damage respectively - were selected based on relevance. These two assets were given special attention for cybersecurity because they are assets that are oftentimes ignored by many organizations implementing cybersecurity solutions. SQL Poisoning could use the website to access a login page to use as a launchpad against Johnson & Johnson as a whole, escalating access to either company secrets or stolen administrative permissions to be used for illicit purposes. Weather damage meanwhile is a different sort of threat. One that does not target any assets, which also means that it does not discriminate in what it could damage. The perceived rarity of extreme weather in the Mid-Atlantic state of New Jersey where Johnson & Johnson could lead to looser standards of construction to prepare for weather events. This is why Johnson & Johnson must conduct independent assessments of the security of its physical facilities in the face of extreme weather.

By taking steps to protect itself against SQL poisoning and extreme weather, Johnson & Johnson can greatly improve its cybersecurity stance. This will not only have the immediate effect of reducing the likelihood of a critical incident where data is either corrupted, lost, or stolen, it will also have the effect of boosting investor confidence. Implementation, as outlined in the report, should not take much time or money. These three factors make Johnson & Johnson implementing the cybersecurity recommendations outlined in this report an obviously beneficial path to take.