White Paper - Learning from The Cybersecurity Attack on Stryker's Microsoft Environment

On March 11, 2026 Stryker, a global medical technology company operating in roughly 60 countries, reported a cybersecurity attack that was disrupting its global Microsoft environment.

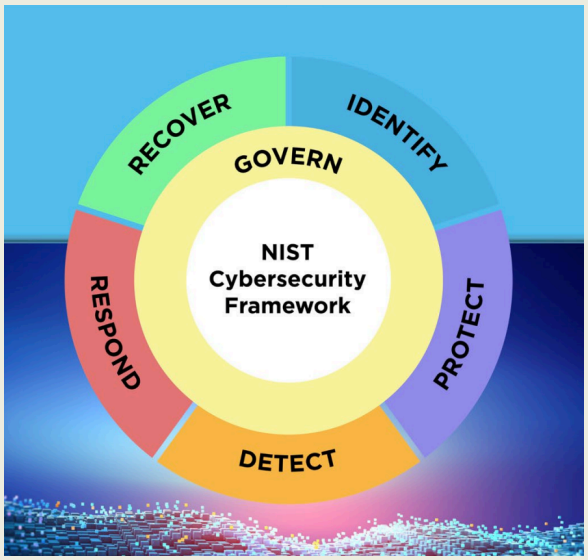
The company impacts more than 150 million patients annually, and had $25.1 billion in 2025 global sales. Against that backdrop, Stryker's March 2026 cyberattack had a significant operational dimension. The company reported a global disruption to its Microsoft environment and later identified impacts to order processing, manufacturing, and shipping, while repeatedly stating that its products, including connected and life-saving technologies, remained safe to use.

Here's a summary of the information about the attack that was published by Stryker on their website:

- March 11, 2026 - Stryker reports global Microsoft environment disruption from cyberattack
- March 12, 2026 12:32 a.m. ET - Incident contained; no indication of ransomware or malware
- March 12, 2026 10:43 a.m. ET - Mako systems confirmed safe for continued use
- March 12, 2026 2:24 p.m. ET - LIFEPAK and LIFENET services confirmed operational
- March 12, 2026 9:13 p.m. ET - Order processing, manufacturing, and shipping disruptions confirmed
- March 13, 2026 3:11 p.m. ET - SurgiCount and Triton confirmed safe and offline-capable
- March 13, 2026 3:13 p.m. ET - Sage ordering disruption continues; backlog planning underway
- March 13, 2026 3:23 p.m. ET - Sustainability Solutions collections continue with possible minor interruptions
- March 13, 2026 3:30 p.m. ET - Endoscopy and Connected OR products confirmed unaffected
- March 13, 2026 5:15 p.m. ET - Vocera and care.ai cloud services confirmed unaffected
- March 13, 2026 6:50 p.m. ET - Stryker reiterates no ransomware or malware indication
- March 15, 2026 11:30 a.m. ET - Product safety confirmed; restoration of ordering and shipping prioritized

There are some valuable insights even small businesses can take away from the incident. One of the most significant is that cloud hosting does not guarantee security and availability. There are practical information security steps that need to be taken.

Enter the NIST Cybersecurity Framework (CSF) and SOC 2 Audits



The NIST Cybersecurity Framework, currently at version 2.0, *"provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes."*

Govern, Identify, Protect, and Detect are continuous activities, while Respond and Recover should be ready when incidents occur. NIST explicitly says the CSF Functions should be addressed concurrently and that Respond and Recover should be ready at all times.

While there's no direct evidence the CSF was used by Stryker it's still possible to see the value of the NIST Cybersecurity Framework in responding to incidents using this incident as a point of reference.

SOC 2 audits have become "table stakes" for winning business with larger prospects and keeping them after winning their business. A SOC 2 type II audit is valuable because it helps validate that controls are well designed, in place and operating

effectively. Taking a step back, how does a small organization quickly go from zero to SOC 2?

The NIST CSF is valuable because it gives organizations a practical structure for asking the right questions and then designing and operating suitable controls. An organization must first be able to answer questions posed by the CSF: What matters most? What systems and data are involved? What controls are in place? How was the incident detected? What was contained? What can continue operating? What must be restored first?

Observing CSF functions as the Stryker incident unfolds

By analyzing Stryker's response to the incident one can observe how the CSF can serve as a functional guide for incident readiness and response. Because the NIST CSF provides tools for organizations, both large and small, the type of process discipline apparent in Stryker's response to the incident is within the reach of small organizations. It is designed to allow organizations to build out practical information security programs that will be effective when real world crises crop up.

Before an incident: Govern / Identify / Protect

Governance is not just policy. Governance is the pre-incident work that lets the organization know what matters, who is responsible, which systems support critical functions, what controls exist, and how the organization will make decisions when normal operations are disrupted.

Stryker's public cybersecurity page gives several useful pre-incident indicators. Stryker says its cybersecurity program:

- Includes a Tier 1 and Tier 2 Security Operations and Cyber Fusion Center that monitors and detects threat activity 24/7
- References risk management, compliance assurance, regulatory and audit functions, product security teams, and a global incident response plan.
- Conducts quarterly security-related exercises and includes internal and external security reviews, security by design, and privacy by design in its Quality Management Program.

What conclusion can we draw about governance from this information? A public trust page or SOC 2 report helps customers understand a product environment. The CSF

provides a broader operational view: products, corporate systems, identity, ordering, shipping, manufacturing, customer support, and recovery.

The NIST CSF During an Incident response

March 11: Detect / initial Respond

Stryker reported a global network disruption to its Microsoft environment resulting from a cyberattack, said there was no indication of ransomware or malware, believed the incident was contained, and said teams were working to understand the impact.

Small organizations often rely on the ad hoc knowledge of systems held by technical staff. The practical value of the framework is that it turns cybersecurity from a set of disconnected technical tasks into a preparation model that helps the business know what it owns, what it depends on, how it is protected, and how it will act when those protections are tested.

Stryker was able to answer the important questions: What environment is affected? What systems are involved? What is still safe to use? What business functions are disrupted? The ability to answer these questions is clearly tied to the Identify tasks in the CSF.

The CSF can help a small organization prepare to answer these same questions as they start to build out their security program. The CSF says assets including “data, hardware, software, systems, facilities, services, people” should be identified and managed based on their importance to the organization. Especially useful subcategories are:

- ID.AM-02, inventories of software, services, and systems
- ID.AM-03, authorized network communications and network data flows
- ID.AM-05, prioritizing assets by classification, criticality, resources, and mission impact
- ID.AM-07, inventories of data and metadata

Using Stryker as an example it is possible to see that all of these CSF elements are highly valuable to launching an organized and coherent response to an intrusion or suspected intrusion.

March 12: Respond / Contain / Communicate

Stryker said that upon detecting the incident it activated its incident response plan, launched an investigation with external advisors and cybersecurity experts, contained the incident to its internal Microsoft environment, implemented business continuity measures, and began collaborating with law enforcement and government partners.

Stryker's statement reflects several practical CSF outcomes: detecting and analyzing an adverse event, activating incident management processes, investigating with external experts, containing the incident, communicating with law enforcement and government partners, and using business continuity measures to support recovery.

While startups, scaleups and small businesses may not require the same level of involvement with law enforcement and government processes there are a number of CSF elements that can help organizations respond to, contain and communicate the impact of security events. Leveraging CSF to design controls and SOC 2 audits to validate controls and ensure their continued effectiveness paves the way for the same level of readiness observable in the Stryker incident:

- DE.AE, Adverse Event Analysis
- RS.MA, Incident Management
- RS.AN, Incident Analysis
- RS.CO, Incident Response Reporting and Communication
- RS.MI, Incident Mitigation
- RC.RP, Incident Recovery Plan Execution

March 12-13: Identify / Protect / Detect / Respond / Recover Cycle

Stryker issued product-specific clarifications for Mako, LIFEPAK, LIFENET, SurgiCount, Triton, Vocera, care.ai, Connected OR, and other platforms. It repeatedly explained whether products were connected, independent, isolated, cloud-hosted, offline-capable, or safe to continue using.

Stryker's product-specific updates reflect several CSF outcomes in practice: maintaining enough asset and architecture knowledge to understand product exposure, using resilient design to limit impact, analyzing which platforms were affected or isolated, and communicating that information in practical terms customers could act on.

Effective governance comes from a collaboration between technical and business leadership. Governing documents should be seen as requirements, guidelines and standards set by the business in general terms. Implementers should be able to use the governance documents to carry out their mission - to identify assets, protect them, detect intrusions and control failures, respond to security events and recover from incidents.

Organizations striving to move from ad hoc security to a more disciplined and demonstrable program can leverage the following CSF elements:

- **Identify - ID.AM, Asset Management:**
  The product-by-product clarification shows the value of knowing which platforms exist, how they are hosted, whether they are connected, and how

they relate to affected environments. That aligns with asset inventories, network/data-flow understanding, and asset criticality.

- **Protect - PR.IR, Technology Infrastructure Resilience:**
  Explaining that some products were independent, isolated, cloud-hosted, or offline-capable supports the idea that architecture and infrastructure design can limit blast radius and preserve service availability.
- **Detect - DE.CM, Continuous Monitoring; DE.AE, Adverse Event Analysis:**
  The ability to distinguish affected from unaffected products depends on monitoring, analysis, and understanding whether observed activity actually indicates risk to a specific platform.
- **Respond - RS.AN, Incident Analysis:**
  Stryker's statement reflects scoping - determining what was affected, what was not, which environments were connected, and whether continued product use was safe.
- **Respond - RS.CO, Incident Response Reporting and Communication:**
  The repeated product-specific updates are a clear communication activity. They translate technical scoping into customer-relevant guidance: "Is my product affected, connected, isolated, or safe to use?"
- **Recover - RC.CO, Incident Recovery Communication:**
  Where Stryker explained that products remained safe to use or offline-capable, that also supports recovery communication: helping customers continue operations with confidence while the incident response continues.

March 13-15: Recover / Prioritize restoration

Stryker said it was prioritizing restoration of systems directly supporting customers, ordering, and shipping. It also said electronic ordering systems were being brought back online and that orders entered before the event would be reconciled.

- **Identify - ID.AM, Asset Management:**
  Prioritizing systems that support customers, ordering, and shipping reflects knowing which systems are most important to business operations and customer impact.
- **Recover - RC.RP, Incident Recovery Plan Execution**
  Bringing electronic ordering systems back online is a direct recovery activity - restoring systems and services after an incident.
- **Recover - RC.CO, Incident Recovery Communication**
  Telling customers which systems are being restored and how orders will be handled maps to recovery communication. It gives affected parties practical information about service status and next steps.

April 1: Recover / Normal operations

Stryker later stated it was fully operational across its global manufacturing network, supported by restored commercial, ordering, and distribution systems.

The endpoint of recovery is more than restoring system availability; it is restored operational capability.

Recover - RC.CO, Incident Recovery Communication

Publicly stating that the global manufacturing network was fully operational is recovery communication. It tells stakeholders not only that systems are back, but that business operations have resumed.

Conclusions for startups and small companies

The CSF is useful because it turns cybersecurity from a pile of controls into an operating model.

For startups, the lesson is not “build a Stryker-scale security program.” The lesson is:

A small company should know:

- which services matter most
- where customer data lives
- which systems support sales, delivery, support, billing, and product operations
- which systems are dependent on Google Workspace, Microsoft 365, AWS, GitHub, Stripe, HubSpot, or other core platforms
- who declares an incident
- who talks to customers
- what gets restored first

It should test those assumptions before the incident.

Stryker’s public updates do not let outsiders audit the company’s cybersecurity program, and that is not the point. The more useful lesson is that the NIST CSF gives organizations a practical way to think before an incident happens. It helps leadership and technical teams ask which services matter, which systems support them, which controls protect them, how incidents are detected, how containment is communicated, and how recovery is prioritized. For startups and small companies, that structure may be the difference between a vague belief that “we have backups” and a practical ability

to keep customers informed, restore critical operations, and make risk-based decisions under pressure.

The ultimate goal of a cybersecurity program should be to support the business in achieving its objectives - selling products and service and keeping customers happy.

***Purple Dragon Cybersecurity** specializes in working with startups, scaleups and small businesses to quickly scale up cybersecurity programs using the CSF and other frameworks. We help prepare these businesses to sell to larger organizations that demand audited security results AND expect them to be prepared to respond to crises.*

Contact us: info@purpledragoncyber.com
