What Stryker's Cyberattack Response Shows About Building a Real Security Program

Release Date: 7 May 2026

When Stryker disclosed a March 2026 cyberattack affecting its global Microsoft environment, the story was not only about a large company experiencing disruption. It was also a useful public example of what a mature security program is supposed to make possible.

Stryker reported that the incident disrupted its Microsoft environment and later affected order processing, manufacturing, and shipping. At the same time, the company repeatedly issued product-specific updates explaining which systems were connected, independent, isolated, cloud-hosted, offline-capable, unaffected, or safe to continue using. It also stated that it activated its incident response plan, brought in external advisors and cybersecurity experts, contained the incident to its internal Microsoft environment, implemented business continuity measures, and coordinated with law enforcement and government partners.

That matters because incident response is not improvised successfully in the middle of a crisis. The ability to say what was affected, what was not affected, which products remained safe, which systems supported customers, and what needed to be restored first depends on preparation.

This is where the NIST Cybersecurity Framework becomes practical rather than theoretical.

The CSF gives organizations a structure for asking the questions that matter before something goes wrong: What assets do we have? Which systems support critical business operations? Where does customer data live? What controls protect those systems? How will we detect problems? Who declares an incident? Who communicates with customers? What gets restored first?

Stryker's public updates do not prove that the company used the CSF, and outsiders should not pretend they can audit Stryker from press statements. But the response clearly illustrates the kind of operational clarity the CSF is designed to support.

The most useful lesson for startups and small companies is not “build a Stryker-scale security program.” It is this: even smaller organizations need a working model for governance, asset management, protection, detection, response, and recovery.

For founders and executives, that model has direct business value. Security is not just a technical function. It supports sales, customer trust, operational continuity, audit readiness, and the ability to survive disruption without losing control of the message.

For security leads and CISOs, the lesson is equally clear. A security program should not be a pile of policies, tools, and compliance tasks. It should help the business answer hard questions under pressure. Which customer services are affected? Which systems can keep operating? Which vendors or cloud platforms are involved? What evidence supports the decision to contain, restore, or communicate?

That kind of readiness is also what larger customers increasingly expect from vendors. SOC 2, ISO 27001, NIST CSF alignment, incident response planning, business continuity, vendor risk management, and executive reporting are no longer just enterprise concerns. They are becoming the price of admission for startups and scaleups that want to sell into serious markets.

The Stryker incident is a reminder that mature organizations do not only invest in prevention. They invest in knowing their environment well enough to respond coherently when prevention is tested.

For smaller organizations, the NIST CSF 2.0 Small Business Quick Start Guide is a good place to begin. But downloading a guide is not the same as building a program. The real work is turning the framework into operating habits: asset inventories, risk decisions, control ownership, monitoring, response plans, recovery priorities, and tested communications.

That is the work Purple Dragon Cybersecurity helps organizations do.

Purple Dragon Cybersecurity works with startups, scaleups, and small businesses to build practical security programs that support growth, customer trust, and audit readiness. We help organizations move from ad hoc security to a structured program using frameworks such as the NIST CSF, SOC 2, and other risk-based approaches.

If your company is starting to face larger-customer security expectations, preparing for SOC 2, formalizing incident response, or trying to understand whether your current controls would hold up under pressure, this is the right time to act.

Download the whitepaper, give it to your security, engineering, and operations teams, and use it as a starting point for a serious internal conversation:

Do we know what matters most?
Do we know what depends on what?
Do we know how we would detect, contain, communicate, and recover?

And if the answer is not clear, Purple Dragon Cybersecurity can help build the program that gets you there.