CYBER SECURITY AND BUSINESS CONTINUITY

SCENARIO 5: AI Goes Rogue

Peter Nielsen smiled as he walked from his car to his office. He was the CEO of Stempelkraft, and the company was enjoying a year of unprecedented publicity, growth and profits. The Jutland-based company designed and manufactured component parts for leading engine manufacturers from the marine, rail and power generation sectors. Stempelkraft's range of products included pistons, piston ring sets, piston pins, and cylinder liners, valves, valve seat inserts and guides, and power cell units designed and sold as customizable complete systems. It was an industry leader in developing composite materials to enhance the durability of cylinder rings and piston pins. For years, it had been a relatively small-scale operation, primarily selling to Nordic and German manufacturing companies. Then, in March 2026, Stempelkraft had competed on, and won, a bid to supply component parts for the new Galaxy-class stealth frigate, the new multi-role warship commissioned by 17 NATO member states' navies. The Galaxy programme made the relatively unknown business into a household name across Denmark, and it was heralded for its innovation and quality.

Peter and the rest of the company board recognized that the Galaxy programme was a great opportunity for Stempelkraft. However, it did present some practical challenges for the business. Stempelkraft had provided power cell units to Danish and Norwegian naval programmes, but it had never undertaken a project of such magnitude and significance before, and staying on top of inventory was proving to be difficult. The business operated across three separate sites and had two separate inventory systems: one for managing incoming components from suppliers, and another for outbound customer orders. Although the warehouse and customer service teams were dedicated and diligent, they were struggling to manage the increased volume and complexity of orders. Considerable time was lost, and many errors made, as the team tried to coordinate inventory using an outdated system that required a lot of manual data input. This needed to be rectified if Stempelkraft was to manage the scale of Galaxy orders.

After consultation with the warehouse and customer service team, the company board made the decision to purchase an AI-enabled inventory management system to streamline and improve processes. Stempelkraft management was confident in the utility and reliability of AI. After all, automation had been integrated into the many aspects of the assembly process, such as piston ring coating and casting of cylinder lining, without issue. AI tools had been steadily growing in both sophistication and popularity since 2020 and were integrated into the inventory management and

customer services interfaces of many similar businesses. In fact, the tool they selected, PowerInventory. Furthermore, it was an approved supplier to the US Navy and therefore met security requirements for the Galaxy programme.

For a medium sized business, PowerInventory was a relatively low-cost way for Stempelcraft to manage a wide range of complex tasks: inventory forecasting, requests, supplier selection, ordering, restocking, transfer, serialization and compliance verification. It had a user-friendly interface for staff and customers, and even a mobile app.

As the months passed, all appeared to be going well. The software implementation had been a surprisingly seamless process, and the warehousing staff had easily adapted to the changes. In fact, they reported that they were working better as a team as situations that had previously caused confusion, or redundant efforts had largely been eliminated. Peter had even managed to highlight the new system in a feature interview with a Danish industry magazine, to show how the company was adapting to meet the demands of an expanded international customer base. After nearly a year of using PowerInventory without incident, the board decided that it was safe to divest of the old inventory software, to reduce the cost of licensing fees of a legacy system that was no longer in use.

Late one Friday afternoon, the warehousing team noticed that it was taking an unusually longtime for the programme to load. Simple requests could not be fulfilled, or timed out unexpectedly, and their computer screens would display 503 ‘service unavailable’ error messages. The team decided that it must be an issue with the company’s internet service provider, or possibly their own mistakes, and left for the weekend, believing that the issue would have resolved itself by Monday morning.

By noon on Monday, however, it appeared that the problem was much more serious than anticipated. Nothing was working. No one could access the system. The customer service team received several calls from clients who reported they were unable to place or review orders either online or on the app. The warehouse team called Stempelkraft’s in-house IT, but they were unable to rectify the problem. The following day, PowerInventory’s head office reported that it had suffered a cyberattack, affecting all its products. The server that Stempelkraft relied upon was unavailable. PowerInventory was working to restore access, but it was unable to estimate when server access might be restored.

Without access to the inventory system, and without their older system, Stempelkraft had no oversight of its inventory, and it was still under contract to deliver orders on time. The board made the decision to halt production until the problem was resolved, while the warehousing and customer service teams created a temporary manual inventory system using Excel spreadsheets. Every nonproductive day cost the company money and delayed product delivery.

Eventually, after three agonizingly expensive weeks, server access was restored, and Stempelkraft was once again able to track its inventory. However, after a month, the warehouse team

noted a recurring issue with serialization. The middle three digits of every serial number were incorrect, making it impossible to trace products accurately. Careful investigation by the warehouse and IT teams determined that the problem could not be traced to a human input error. Somehow, the model had changed its parameters and was now replicating an incorrect pattern. It pointed to a much deeper and more serious problem than a few numbers out of sequence. Peter feared that , with the inventory system so seriously compromised, Stempelkraft could lose the Galaxy contract altogether.

AI Goes Rogue **Potential risks for business**
1. What are the key risk factors and vulnerabilities in this scenario?
2. What risks does this scenario pose to Danish businesses?
3. What vulnerabilities affect your business?
4. What mitigation, if any, has your business considered or implemented?

03.09.2025: Prepared in the project Cybersecurity and Business Continuity in small and medium-sized Danish manufacturing companies. The project is funded by the Danish Industry Foundation.