ARMADA
Powered by risk3sixty

# RED TEAMING ELEVATES SECURITY IN EMBECTA'S COMPLEX IT ENVIRONMENT

## Defense Based On Mimicking Real-World Attacks

- Navigating the complexities of their robust IT systems
- The Red Team mission that challenged their IT and physical security
- Insights that helped harden their security posture

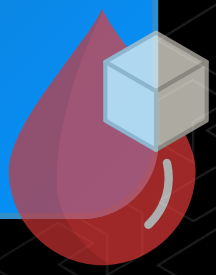
# NAVIGATING THE COMPLEXITIES

**embecta Corp., aka embecta, is a prominent provider of diabetes products in the United States and across the globe.**

**As a recent spin-off from a larger conglomerate, the company encountered various challenges while integrating new systems and managing legacy devices and infrastructure.**

These challenges created a complex IT environment requiring enhanced control and security measures. To address these challenges, embecta partnered with risk3sixty for a comprehensive red teaming engagement.

The goal was to identify potential risk in embecta's IT infrastructure and security practices, evaluating their defenses against potential real-world attacks.



**After spinning off from its former parent, embecta faced the task of managing overlapping legacy systems and processes.**

This situation led to challenges with its employees, who needed to continue using legacy systems and infrastructure for a period of time. The limited control over these systems posed a security risk, as embecta had to ensure that all IT assets were correctly managed and secured.

**The use of legacy devices and infrastructure posed a challenge in maintaining a secure IT environment.** The company also needed to distinguish and transition to new systems while ensuring continuous, secure operations.

**With a significant international footprint, the company relies on numerous third-party vendors to manage its infrastructure.** Third parties can lead to inconsistencies in security protocols and control measures, which could introduce new risk.

# THE RED TEAM MISSION

**Risk3sixty's engagement involved simulating attacks using various techniques to accurately reflect potential real-world threats.** The first step was threat actor emulation, where skilled ethical hackers from risk3sixty simulated attacks to identify and exploit vulnerabilities, much like a malicious actor would.

**This approach provided embecta with a realistic view of potential threats and their impact.**

Social engineering and physical security testing were also key components of the engagement. **Techniques such as lock picking, bypassing security systems, and conducting phishing tests were employed to assess the robustness of embecta's physical and IT security measures.** This multifaceted approach ensured that both digital and physical security aspects were thoroughly evaluated.

**The assessment of access control systems included detailed testing of locks, access controls, and surveillance systems to identify weaknesses that could be exploited for unauthorized access**. This helped embecta understand potential entry points and weaknesses in their physical security infrastructure.

**Finally, the engagement involved evaluating embecta's incident response plans.** This assessment ensured that responses to security breaches were swift and effective, providing embecta with insights into improving their incident response strategies and readiness.

# UNVEILING THE INSIGHTS

**The red teaming engagement uncovered enlightening data regarding the security of embecta's IT infrastructure.**

**One finding included an Internet Service Provider (ISP) in the Asia Pac region had not correctly secured a router, providing internet access to a site.** Although this was outside the enterprise network, this issue from the ISP needed to be remediated.

**The engagement also revealed a remote desktop being hosted by a service supplier.** The issue was remediated by the vendor at embecta's request to ensure a secure and well-managed IT environment.

**Physical security was assessed at an embecta site, with a focus on locks and surveillance systems.** Recommendations were provided on how to further secure their physical environments.

**Social engineering attempts were conducted by risk3sixty to test embecta's service desk processes.** Recommendations were provided to help improve protocols to protect user credentials and prevent unauthorized access.

# OUTCOME OF THE ENGAGEMENT

**The outcomes of the engagement provided embecta with essential insights into its security posture.**

By identifying potential risks and providing security recommendations in network management and physical security protocols, embecta was able to further enhance their IT and security policies.

This included strengthening asset management practices and enhancing employee training programs.

# LESSONS LEARNED AND THE PATH FORWARD

**Partnering with risk3sixty allowed embecta Medical LLC to gain a comprehensive understanding of its security landscape.** The red teaming engagement identified potential issues and provided actionable insights to improve embecta's IT and physical security measures.

**By addressing the findings, embecta elevated their security operations to enable an even more secure IT environment.**

# CONTACT US TODAY!


**Cory Wolff**
cory.wolff@risk3sixty.com

**Ross McCurdy**
ross.mccurdy@risk3sixty.com