

## A Compromised Home: The call was coming from inside the house...



### Client Profile

**Name:** Liam\*

**Occupation:** CEO of a large, high-profile insurance company

**Status:** Existing BlackCloak client

### The Challenge

Liam is an existing client of BlackCloak and has been relying on its technologies and services to protect his and his family's digital and physical assets for the last several years. As the CEO of a successful and well-regarded insurance company, Liam became a client because he knew that he couldn't just rely on consumer-grade products and his physical security teams to keep him safe.

Liam needed to add a layer of personal cybersecurity as that was the most likely way cybercriminals would compromise his wealth and his company's security.

BlackCloak worked with Liam's physical security team to ensure that all aspects of his life were protected. This included access to the software and equipment that was constantly monitoring Liam's home.

One component of BlackCloak's service is to conduct weekly home network vulnerability scans, then deeper penetration tests if needed. This ensures that everything is working as it should and there are no gaps in coverage. A penetration test involves simulating cyberattacks against a client's systems to help identify any vulnerabilities that could be potentially exploited. During one of these penetration tests, an open port was found.

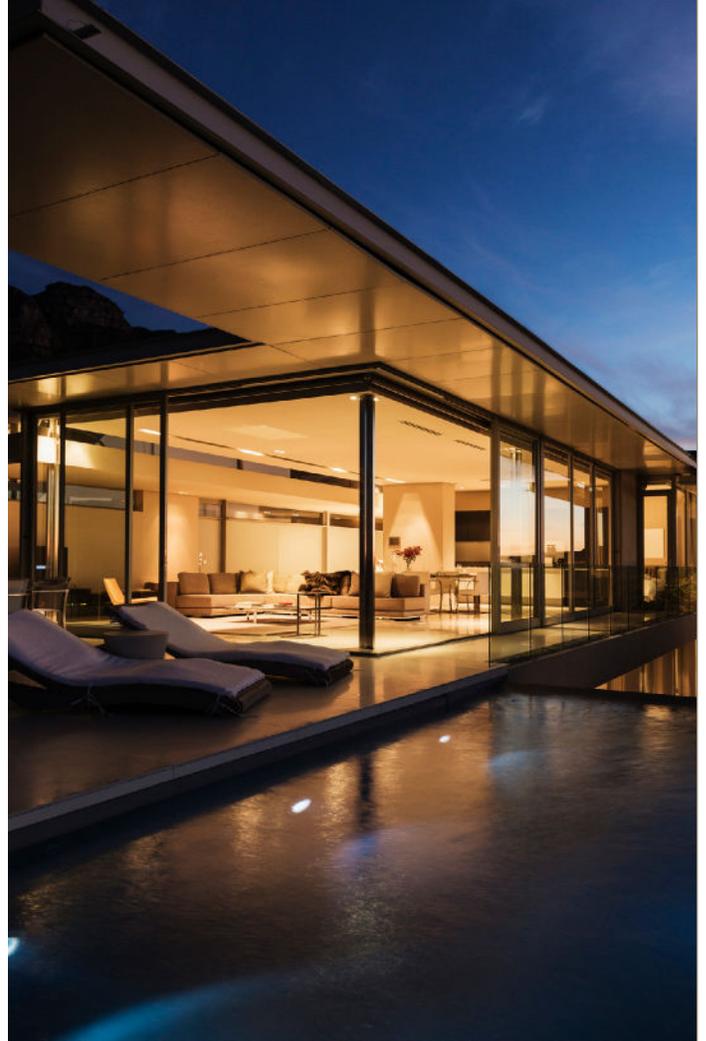
At first, the BlackCloak team could not identify what the port was, as it was transmitting encoded status updates. Because the port was open, it could be manipulated by others that sought access to it. For instance, to test access, BlackCloak's remote team could turn on the lights in Liam's home, as the security system was connected to the home's automation platform. Although no intrusion had occurred, the open, non-secure port presented a serious vulnerability, potentially allowing unauthorized access to Liam's home.

*\*All names (and specific details) have been changed to protect the clients privacy.*

## The Solution

The BlackCloak security team quickly identified the source of the vulnerability and recognized the immediate risk it posed. They discovered that the home security system's graphical interface could be accessed using a default password, further compromising security.

To remediate the issues, the BlackCloak team promptly contacted Liam and his security team with immediate recommendations. The original installation team was brought in to close the open port and change the default password to a secure one. This ensured that the home security system was no longer vulnerable to external threats.



## Results

Through proactive and decisive action, BlackCloak mitigated the potential threat before any intrusion occurred. Liam's home security system is now secure, and he can rest easy knowing that his and his family's digital and physical assets are well protected.

This case highlights the importance of continuous monitoring and proactive measures in maintaining robust cybersecurity, demonstrating BlackCloak's commitment to safeguarding its clients' security.