

CISO Protects Intellectual Property by Securing Executive Devices

Description

- CISO of a pharmaceutical company
- 14 person executive team using personal devices for work
- Growing cyber risk targeting intellectual property



The Problem:

Executive Team Identity Theft

The CISO of a pharmaceutical company was struggling with executives using their personal devices for company work, increasing the cyber risk of identity theft cases. This also resulted in intellectual property and sensitive company data being leaked outside the company's controls.

The CISO suggested extending the same security protections used by the corporation into the homes of the executives and their personal devices to prevent additional risk, but was met with push back.

Needing to protect the company by protecting the executives was a non-negotiable. A new digital executive protection project was rolled out, but before full implementation was reached, the executive team was compromised with identity theft.

BlackCloak Steps In

The CISO worked with BlackCloak to roll out a holistic Digital Executive Protection to all executives. Under BlackCloak's guidance, the CISO was able to roll-out the program with little friction, using short onboarding meetings to ensure the executives program participation, limit the time they were offline from corporate business, and empower them with total control over their accounts.

The first course of action was to remediate the recent identity theft issues. To do so, BlackCloak implemented the following services:

01.

Data broker removal services to prevent social engineering of executives to get at corporate infrastructure

02.

Mobile device and computer hardening to detect and remediate malware and other vulnerabilities that could expose corporate intellectual property.

03.

Weekly home network scans to determine vulnerabilities on the executives' personal routers, in-home automation systems, and across security camera systems.



The Result

*Secured Devices, Remediated Threats,
Protected Company*

The CISO took control of an out of hand situation, ensuring that the personal devices and home networks of his company's executive team thereby protecting the entire company as a result. With help from BlackCloak, the CISO stopped the bleeding of identity theft without draining the company's resources. Because the identity theft was remediated immediately, the risks of having to file disclosures with the SEC or announce publicly have been mitigated.

BlackCloak removed data broker information, changed exposed passwords, and put credit monitoring in place. Now, any existing malware has been remediated and the executive team's personal mobile devices and computers have BlackCloak installed for ongoing monitoring and protection.