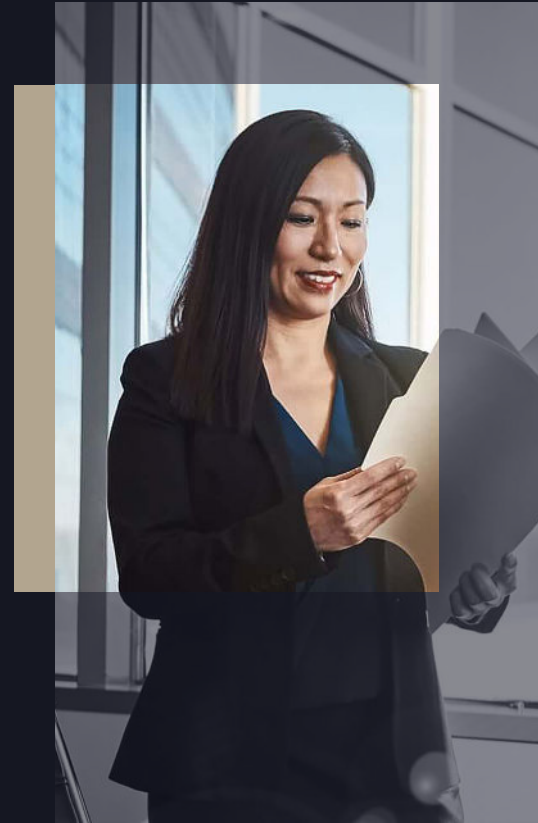


Protecting Executives Personal Information in the Wake of a Cyberattack

Description:

- Life Sciences company
- Intellectual Property to protect
- 12+ member executive team
- General Counsel leading effort to implement improved protections



The Problem:

Personal Data Stolen from Corporate Systems

A Life Sciences company was a victim of a ransomware incident, resulting in its executive team and their assistant's highly personal information (passport numbers, SSN, passwords) being exfiltrated from the corporate systems. The company was concerned that the exposure of this sensitive information would put them at risk for loss of intellectual property, data breaches, and reputational impact.

After all, companies are only as secure as their executives.

BlackCloak Steps In

Prior to the ransomware incident, the General Counsel had been working on a digital executive protection project and the incident spurred him to accelerate its progress.

As a result, the company purchased BlackCloak's executive cybersecurity protection plans that included identity theft and fraud protection for the entire executive team and assistants. It was quickly rolled out to the new members, securing their personal devices, monitoring device and account activity, home network security scans, and scanning the deep and dark web for exposed passwords.

With BlackCloak's help, all executives enabled multi-factor authentication (MFA) on email, bank, and social media accounts to prevent future breaches. In addition to putting credit monitoring in place, identity theft insurance up to \$1 million was included in each plan.



Set minds at ease by personalizing the response to their specific needs and give them control by not using corporate controls and personnel.



The Result

Protected company reputation and bottom line while preventing future hacking attempts.

By partnering with BlackCloak early, the General Counsel accelerated the post-breach remediation. The General Counsel and CISO had BlackCloak apply executive cybersecurity protection to secure the executive team's personal devices including installing anti-malware software on devices shared with family members. The company's CISO and General Counsel are now receiving aggregated, anonymized reports on protection status. Thanks to these additions, when an executive's personal social account was hacked six months later, the situation was detected and mitigated immediately.