



AN INTERVIEW WITH DR. CHRIS PIERSON,
FOUNDER AND CEO, BLACKCLOAK

CONCIERGE DIGITAL PROTECTION FOR CORPORATE EXECUTIVES AND HIGH-ACCESS EMPLOYEES FROM BACKCLOAK

An executive's digital footprint and online presence is one of the new attack surface vectors into a targeted enterprise. The personal devices and home networks of corporate leaders are often not protected, requiring new security solutions to address this risk to avoid attacks on a company.


To minimize cybersecurity risk, BlackCloak provides concierge digital executive protection for upper management, board members and high-risk employees, along with their families. We wanted to better understand the risks originating from personal digital lives, as well as BlackCloak's comprehensive SaaS-based solution that addresses the security and privacy concerns of its clients.

TAG Cyber: How can companies be targeted through the digital presence of their executives?

BLACKCLOAK: The soft underbelly of enterprise security has become the personal digital lives of key employee personnel—in particular, those with access to corporate strategy, confidential information, proprietary data and finances. This is partly due to the normalization of remote and hybrid work, but is mostly the result of cybercriminals identifying a new path of least resistance, allowing them to seamlessly bypass a company's robust security controls. CISOs have done a great job in hardening the corporate environment, and now personal digital lives—including digital privacy, personal devices and home networks—have become the next weakness. We know from our own data that more than three-in-ten executives have malware on their personal devices, while 23% have open ports on their home networks. Additionally, 87% of personal devices are leaking data, and only 8% have MFA installed across all apps, devices and systems. Not to mention, a majority of people still use the same passwords in their personal and professional lives.

All of this presents a huge problem to a company for a variety of reasons. For one, attackers who successfully breach a home network or personal email often have unobstructed green space to move laterally into an organization's digital infrastructure and launch a malware or ransomware attack. Earlier this year, US cybersecurity officials caught Chinese nation-

CISOs have done a great job in hardening the corporate environment, and now personal digital lives—including digital privacy, personal devices and home networks—have become the next weakness.



state hackers doing this very thing with the personal Gmail accounts of high-value workers in critical infrastructure. Many busy executives conduct professional work on personal devices. A breach of any personal device can lead to direct and collateral damage to a business, primarily in the form of financial fraud, reputation damage, business email compromise, account hijacking, unauthorized access and other impacts of consequence. Cybercriminals know that personal devices are highly susceptible to cyberattack and there is very little security teams can do on their own to mitigate this risk; corporate controls cannot be extended into personal lives, due to resource, legal, privacy and ethical constraints, and consumer-grade protections aren't built to withstand advanced targeted attacks.

TAG Cyber: How does the BlackCloak offering work?

BLACKCLOAK: We provide complete, enterprise-grade, digital privacy protection, home-network security, personal device security for mobile and desktop, and incident response via a single SaaS-based platform. Our proprietary technology helps reduce the digital footprint of corporate leaders by removing their personal information from more than 200 data-broker websites. We also scan the deep and dark webs daily for compromised accounts and passwords. We harden privacy settings across all devices, apps and systems to help protect the location and identity of our customers. On devices, we provide XDR technology via an intuitive application that is of a similar caliber to what can be found on corporate phones and computers. We scan devices for botnets and have created our own deception network to trick and trap potential adversaries across all member endpoints. We protect the home through weekly penetration tests, in search of open ports and compromised Wi-Fi. All our technology is backed by a US-based security operations center, offering 24/7 incident response every day of the year. Our white-glove concierge support service answers all customer questions and navigates challenges, while creating a culture of privacy and security.

TAG Cyber: How does your solution work for families?

BLACKCLOAK: Cybercriminals don't care who they hack, as long as it helps them achieve their objectives. Thus, family members of corporate leaders are increasingly at risk. Every week, our team sees a spouse or partner being targeted in an effort to attack the main executive target. And if you think kids are off limits, think again. We protect family members in the same way we protect our corporate clientele.

TAG Cyber: Tell us more about how enterprise teams can engage with you to protect their leaders.

BLACKCLOAK: Most companies recognize that there needs to be a separation between the personal and private lives of

their executives, due to legal, ethical, compliance and privacy concerns. Nonetheless, there are risks that need to be mitigated. When a company decides to use BlackCloak, a set amount of executives, and sometimes their family members, then become BlackCloak members, and we become responsible for their security. To ensure privacy, we never share any personal information with the company. Security teams receive monthly updates from their account rep that are aggregated and anonymized, providing them with an overview of the threat landscape of their executives without having direct visibility into any one person or occurrence. If there is an incident, we collaborate with the corporate security team, providing them with the required information so they can protect the company without compromising an executive's privacy.

TAG Cyber: Can you share some insight into the future of personalized cybersecurity in the coming years?

BLACKCLOAK: We believe that the future of executive protection is digital. As the line between the physical and digital worlds becomes all but indistinguishable, we know that personal cybersecurity will quickly escalate in enterprise and mid markets, going from something that's nice to have to an urgent need. We've already seen this starting to occur; companies that didn't view personal digital lives as an attack vector a year ago are now customers. In addition, we believe that expanded attack surfaces will compel greater collaboration between CISO-led digital security teams and a CSOs physical security teams. After all, ensuring physical security can no longer be accomplished without visibility into the virtual, and vice versa. We also believe that for executive cybersecurity to mature as an industry, it must prioritize privacy by offering the kind of bespoke customer support that high-value individuals are accustomed to in all other facets of their lives.

